Université Mohamed V- Agdal
Faculté des Sciences
Département de Mathématiques
Avenue Ibn Batouta, B.P. 1014, Rabat Maroc.

Filières SM et SMI

Algèbre 4

STRUCTURES ALGEBRIQUES

AZZOUZ CHERRABI ELMOSTAFA JABBOURI

Année 2007-2008

Table des matières

Chapitre 1

Arithmétique

1.1 Les entiers naturels

1.1.1 Définitions

Définition 1.1 *Les cardinaux finis (ou cardinaux des ensembles finis) sont appelés* ***entiers naturels****. Leur ensemble, noté* $\mathbb{N}$*, contient donc l'élément particulier 0 et est muni d'une application* $S : \mathbb{N} \longrightarrow \mathbb{N}$*, appelée successeur, ou* ***fonction succession****, satisfaisant aux axiomes suivants (Dedekind, Peano) :*

(S1) S *est injective*

(S2) $0 \notin S(\mathbb{N})$

(S3) $\mathbb{N}$ *est l'unique partie de* $\mathbb{N}$ *contenant* 0 *et stable par* S*.*

Remarque 1.2 0 *est l'unique élément de* $\mathbb{N}$ *qui n'est le successeur d'aucun élément de* $\mathbb{N}$*. i.e.,* $\{0\} \cup S(\mathbb{N}) = \mathbb{N}$*. En effet, posons* $E = \{0\} \cup S(\mathbb{N})$*,* $E \subset \mathbb{N}$ *et* $0 \in E$*. On a aussi, si* $x \in E$*, alors* $x \in \mathbb{N}$ *et ainsi* $S(x) \in E$*. En utilisant (S3), on a* $E = \mathbb{N}$*, i.e.,* $\{0\} \cup S(\mathbb{N}) = \mathbb{N}$*.*

1.1.2 Opérations dans $\mathbb{N}$ et Raisonnement par récurrence

On définit successivement **l'addition** sur $\mathbb{N}$ par : $m + 0 = m$, $m + S(n) = S(m + n)$, (il s'en suit alors que, si $1 = S(0)$, $m + 1 = m + S(0) = S(m + 0) = S(m)$), la **multiplication** par : $m.0 = 0$ et la formule récurrente $m(n + 1) = mn + m$.

Théorème 1.3 (Théorème de récurrence) *Si*

(i) 0 *possède une propriété* P *et*

(ii) $P(n)$ *est vraie entraine* $P(n + 1)$ *est vraie*

alors tous les entiers naturels possèdent la propriété P*.*

Preuve. Pour établir ce théorème, Il suffit d'utiliser (S3) en posant $E = \{n \in \mathbb{N}/P(n)$ est vraie$\}$ ■

Exemple 1.4 *Montrons par récurrence que* $\forall n \in \mathbb{N}$, $1.1! + 2.2! + ... + (n + 1).(n + 1)! = (n + 2)! - 1$*. En effet, posons* $f(k) = 1.1! + 2.2! + ... + (k + 1).(k + 1)!$*, alors* $f(0) = 1 = (0 + 2)! - 1$*. Supposons que* $f(k) = (k + 2)! - 1$*, on a alors,* $f(k + 1) = 1.1! + 2.2! + ... + (k + 1).(k + 1)! + (k + 2)(k + 2)! = f(k)+(k+2)(k+2)! = (k+2)!-1+(k+2)(k+2)!$*. Ainsi,* $f(k+1) = (k+2)!(1+k+2)-1 = (k+3)!-1$*. D'où,* $f(n) = (n + 2)! - 1, \forall n \in \mathbb{N}$*.*

Théorème 1.5 *L'addition et la multiplication possèdent les propriétés suivantes : pour tous* $m, n, k \in \mathbb{N}$*, on a :*

(i) $(m + n) + k = m + (n + k)$

(ii) $m + n = n + m$ *(cardinal d'une union disjointe)*
(iii) $m + n = 0$ *si, et seulement si,* $m = n = 0$
(iv) $m(nk) = (mn)k$
(vi) $mn = nm$ *(cardinal du produit de deux ensembles)*
(vii) $m(n + k) = mn + mk$
(viii) $mn = 0$ *si, et seulement si,* $m = 0$ *ou* $n = 0$

Preuve. Montrons, par exemple, la propriété (i) (associativité de l'addition dans $\mathbb{N}$). Effectuons une récurrence sur k. Si $k = 0$, on a $(m+n)+0 = m+n = m+(n+0)$. Supposons l'égalité établie pour k. Alors, par définition de l'addition et d'après l'hypothèse de récurrence, on a $(m + n) + (k + 1) = (m + n) + S(k) = S((m + n) + k)) = ((m + n) + k) + 1 = (m + (n + k)) + 1 = S(m + (n + k)) = m + S(n + k) = m + (n + S(k)) = m + (n + (k + 1))$ ■

1.1.3 Relation d'ordre dans $\mathbb{N}$

Théorème et Définition 1.6 *La relation notée* $\leq$ *et définie sur* $\mathbb{N}$ *par* $\forall a, b \in \mathbb{N} : a \leq b$ *si, et seulement si, il existe* $t \in \mathbb{N}$ *tel que* $b = a + t$ *est une relation vérifiant les propriétés suivantes :*
(i) $\leq$ *est une* ***relation d'ordre total****, i.e.,* $\leq$ *est reflexive, antisymétrique, transitive et pour tous* $m, n \in \mathbb{N}$*, on a* $m \leq n$ *ou* $n \leq m$
(ii) $\leq$ *est compatible avec l'addition, i.e.,* $\forall m, n, p \in \mathbb{N}$, $m \leq n$ *si, et seulement si,* $m + p \leq n + p$
(iii) $\leq$ *est compatible avec la multiplication par un entier non nul, i.e.,* $\forall m, n \in \mathbb{N}, \forall p \in \mathbb{N}^*$, $m \leq n$ *si, et seulement si,* $mp \leq np$

Preuve. Montrons par exemple que $\forall m, n \in \mathbb{N}$, $m \leq n$ ou $n \leq m$. Effectuons une récurrence sur m. Si $m = 0$ alors $\forall n \in \mathbb{N} : 0 \leq n$ (car $n = 0 + n$). Supposons que cette propriété est vraie pour l'entier m. Soit $n \in \mathbb{N}$, distinguons les deux cas suivants :
- $n = 0$ et alors $n \leq m + 1$
- $n \neq 0$, considérons alors le prédécesseur de n, i.e., l'entier n' tel que $n = S(n') = n' + 1$. En utilisant l'hypothèse de récurrence, on a $m \leq n'$ ou $n' \leq m$ et ainsi :
  * si $m \leq n'$, alors $\exists t \in \mathbb{N} : n' = m + t$, d'où $n = n' + 1 = (m + t) + 1 = (m + 1) + t$ et $m + 1 \leq n$.
  * si $n' \leq m$, alors $\exists t \in \mathbb{N} : m = n' + t$, d'où $m + 1 = n' + t + 1 = (n' + 1) + t = n + t$ et $n \leq m + 1$ ■

Remarque 1.7 *La forme suivante du théorème 1.3, dite* ***récurrence généralisée****, est souvent utilisée :*
Soit $P(n)$ *une propriété dépendant d'un entier naturel* n*.* ***Si***
(i) $P(0)$ *est vraie et*
(ii) $\forall n \in \mathbb{N}$, *(*$\forall m \leq n, P(m)$ *vraie) entraine* $P(n + 1)$ *vraie,* ***alors***
$P(n)$ *est vraie pour tout entier* n*.*
Pour la démonstration, on considère cette fois ci la propriété $Q(n) = P(0)$ *et* $P(1)$ $\ldots$ *et* $P(n)$ *et on utilise le théorème de récurrence.*

D'autres propriétés de $\mathbb{N}$ s'avèrent très utiles dans la pratique :

Proposition 1.8
(i) $\mathbb{N}$ *possède un plus petit élément (qui est évidement 0) et toute partie non vide de* $\mathbb{N}$ *admet un plus petit élément.*
(ii) Soit A *une partie non vide de* $\mathbb{N}$*. Alors, les propositions suivantes sont équivalentes :*
a) A *possède un plus grand élément*
b) A *est majorée*

c) A est finie.
(iii) $\mathbb{N}$ n'est pas majoré.
*(iv) $\forall (a,b) \in \mathbb{N}\times\mathbb{N}^*$, $\exists n \in \mathbb{N}$ tel que $nb > a$ (**Propriété d'Archimède**)*

Preuve. Montrons par exemple la propriété (i) : considérons une partie A de $\mathbb{N}$ ne possédant pas de plus petit élément et montrons que A est vide. Soit $P(n)$ la propriété « aucun entier $\leq n$ n'est dans A ». Si $m \in A$ alors $P(m)$ est fausse (car $m \leq m$ et $m \in A$).

$P(0)$ est vraie : sinon $0 \in A$ et ainsi 0 est le plus petit élément de A. Supposons que $P(k)$ est vérifiée et que $P(k+1)$ est fausse. Il existe alors un entier $j \leq k+1$ appartenant à A. Comme $P(k)$ est vraie (aucun entier $\leq k$ n'est dans A), $k+1 \in A$ et ainsi $k+1$ est le plus petit élément de A. Par conséquent, $P(k+1)$ est vraie et $P(n)$ est donc vraie $\forall n \in \mathbb{N}$, ainsi $A = \emptyset$ ■

Conséquence 1.9 $\forall (a,b) \in \mathbb{N}\times\mathbb{N}^*$ $\exists! q \in \mathbb{N} : bq \leq a < b(q+1)$.

Preuve. Si $B = \{n \in \mathbb{N}/\ nb > a\}$, alors, d'après la propriété (iv) de la propositon précédente, $B \neq \emptyset$ et ainsi, en utilisant la propriété (i) de la même proposition, B possède un plus petit élément qu'on note $q+1$ et $bq \leq a < b(q+1)$. L'unicité de q est triviale ■

1.2 Entiers relatifs

Rappelons que l'addition dans $\mathbb{N}$ n'est pas une loi de groupe, mais elle est commutative, associative et tout élément est régulier. On peut donc construire le symétrisé de $\mathbb{N}$, on le note $\mathbb{Z}$ et ses éléments sont appelés des entiers **rationnels** ou **relatifs** (cf. Exercice 1.10). Il est muni d'une addition et d'une multiplication prolongeant celles de $\mathbb{N}$.

Les propriétés de ces deux lois permettent de munir $\mathbb{Z}$ d'une structure d'anneau intègre (cf. chapitre III). $\mathbb{Z}$ est aussi totalement ordonné par la relation $x \leq y$ si, et seulement si, $y - x \in \mathbb{N}$ qui prolonge l'ordre de $\mathbb{N}$.

Exercice 1.10 (Constuction de $\mathbb{Z}$) *Soit $\mathcal{R}$ la relation définie dans $\mathbb{N}\times\mathbb{N}$ par : $(a,b)\mathcal{R}(a',b')$ si, et seulement si, $a + b' = a' + b$.*

1) Vérifier que $\mathcal{R}$ est une relation d'équivalence sur $\mathbb{N}\times\mathbb{N}$

2) On note $\mathbb{Z}$ l'ensemble quotient $(\mathbb{N}\times\mathbb{N})/\mathcal{R}$. Vérifier que si $\overline{(a,b)}, \overline{(a',b')} \in \mathbb{Z}$, alors $\overline{(a+a', b+b')}$ ne dépend que des classes d'équivalence $\overline{(a,b)}$ et $\overline{(a',b')}$ et non du choix des représentants (a,b) et (a',b') de ces classes. Ainsi, on définit l'addition dans $\mathbb{Z}$ comme suit : $\overline{(a,b)} + \overline{(a',b')} = \overline{(a+a', b+b')}$.

3) Montrer que $(\mathbb{Z}, +)$ est un groupe abélien.

4) Soit l'application $\varphi : \mathbb{N} \longrightarrow \mathbb{Z}$ définie par : $\varphi(a) = \overline{(a,0)}$. Montrer que φ est injective et que $\forall a,b \in \mathbb{N}$, $\varphi(a+b) = \varphi(a) + \varphi(b)$.

5) Vérifier que $\forall \overline{(a,b)} \in \mathbb{Z}$ tel que $a \geq b$ (resp. $a \leq b$) $\exists! c \in \mathbb{N} : \overline{(a,b)} = \overline{(c,0)}$ (resp. $\overline{(a,b)} = \overline{(0,c)}$). (On note $\mathbb{Z}_+$ (resp. $\mathbb{Z}_-$) l'ensemble des classes $\overline{(a,b)}$ telles que $a \geq b$ (resp. $a \leq b$) et à l'aide de l'injection φ, on peut identifier $\mathbb{N}$ à $\mathbb{Z}_+$ et ne pas faire de distinction entre $a \in \mathbb{N}$ et $\varphi(a) \in \mathbb{Z}_+$).

Exercice 1.11 *Montrer que*

1) Les éléments inversibles pour la multiplication dans l'anneau $\mathbb{Z}$ sont 1 et -1.

2) Toute partie non vide et majorée (resp. minorée) de $\mathbb{Z}$ possède un plus grand élément (resp. un plus petit élément). (Ind : Soient A une partie non vide et majorée de $\mathbb{Z}$, $a \in A$ et M un majorant de A. On considère $N = \{n \in \mathbb{N}/\ a+n \in A\}$. Vérifier que N possède un plus grand élément m et montrer que $a+m$ est le plus grand élément de A).

3) $\forall (a,b) \in \mathbb{Z}\times\mathbb{Z}^*$, $\exists n \in \mathbb{Z}$ tel que $nb > a$ (Propriété d'Archimède)

4) $\forall (a,b) \in \mathbb{Z}\times\mathbb{N}^*$, $\exists! q \in \mathbb{Z}$ tel que $bq \leq a < b(q+1)$.

1.3 Divisibilité dans $\mathbb{Z}$

1.3.1 Définition et Propriétés

Définition 1.12 *Soient a et b deux entiers relatifs quelconques. On dit que a* ***divise*** *b et on écrit* ***a/b*** *s'il existe un entier $k \in \mathbb{Z}$ tel que $b = ka$.*

Proposition 1.13 *Pour tous a, b, c éléments non nuls de $\mathbb{Z}$,*
(i) a/a
(ii) Si a/b et b/a alors $a = b$ ou $a = -b$
(iii) Si a/b et b/c alors a/c
(iv) Si a/b et a/c alors $a/b + c$

Théorème 1.14 (Théorème de la Division Euclidienne) *Soit $(a, b) \in \mathbb{Z}\times\mathbb{Z}^*$, alors il existe un couple (q, r) unique d'entiers relatifs vérifiant : $a = bq + r$ et $0 \leq r < |b|$.*

Preuve. La division euclidienne est une conséquence du fait que $\mathbb{Z}$ est archimédien :

Existence : Si $b > 0$, on considère l'entier q tel que $bq \leq a < b(q+1)$ (cf. la propriété 4 de l'exercice 1.11) et l'entier $r = a - bq$. Si $b < 0$, alors, d'après ce qui précéde, $\exists q_1, r \in \mathbb{Z} : a = q_1(-b) + r$ avec $0 \leq r < |b|$ et ainsi il suffit de prendre le couple $(-q_1, r)$.

Unicité : Soient (q, r) et (q', r') deux couples d'entiers tels que $a = bq + r$, $0 \leq r < |b|$ et $a = bq' + r'$, $0 \leq r' < |b|$, alors $b(q - q') = r' - r$ d'où $|b|\,|q - q'| = |r - r'|$. D'autre part, on a $|r - r'| < |b|$ car $0 \leq r < |b|$ et $0 \leq r' < |b|$. Ainsi, $|b|\,|q - q'| = |r - r'| < |b|$ et par conséquent $|q - q'| = 0$, i.e., $q = q'$ et $r = r'$ ■

Corollaire 1.15 (Division Euclidienne dans $\mathbb{N}$) *Soit $(a, b) \in \mathbb{N} \times \mathbb{N}^*$, alors il existe un couple (q, r) unique d'entiers naturels vérifiant : $a = bq + r$ et $0 \leq r < b$.*

Preuve. Supposons que $a \geq b$ (si $a < b$ on pose $r = a$ et $q = 0$), alors $a > r$ et ainsi $q \in \mathbb{N}$ (car $bq = a - r \in \mathbb{N}$) ■

1.3.2 Sous-groupes de $\mathbb{Z}$

Notation 1.16 *Soit n un entier relatif, on note $n\mathbb{Z} = \{nm/\ m \in \mathbb{Z}\}$. On a ainsi $\{0\} = 0\mathbb{Z}$ et $\mathbb{Z} = 1\mathbb{Z}$.*

Proposition 1.17
(i) Pour tout entier relatif n, $(n\mathbb{Z}, +)$ est un sous-groupe du groupe $(\mathbb{Z}, +)$.
(ii) Soit $(a, b) \in \mathbb{Z}^2$. a/b si, et seulement si, $b\mathbb{Z} \subset a\mathbb{Z}$.

Conséquence 1.18 *Soit $(a, b) \in \mathbb{Z}^2$, on a $a\mathbb{Z} = b\mathbb{Z}$ si, et seulement si, $a = b$ ou $a = -b$. Ainsi pour tout $a \in \mathbb{Z}$, il existe un unique entier naturel k tel que $a\mathbb{Z} = k\mathbb{Z}, (k = |a|)$. On appelle l'entier k le générateur positif de $a\mathbb{Z}$.*

Théorème 1.19 *Si H est un sous-groupe du groupe additif $(\mathbb{Z}, +)$, alors il existe un unique entier naturel n tel que $H = n\mathbb{Z}$.*

Preuve. Supposons que $H \neq \{0\}$ (si $H = \{0\}$ alors $H = 0\mathbb{Z}$), alors $N = \{m \in \mathbb{N}^*/\ m \in H\}$ est non vide. Soit n le plus petit élément de N et montrons que $H = n\mathbb{Z}$. Puisque $n \in H$, alors $n\mathbb{Z} \subset H$. D'autre part, soit $h \in H$, alors, d'après le théorème de la division euclidienne dans $\mathbb{Z}$, $\exists!(q, r) \in \mathbb{Z}^2 : h = nq + r$ avec $0 \leq r < n$, ainsi $r = h - nq \in H$ et puisque n est le plus petit élément de N, alors nécéssairement $r = 0$ et $H \subset n\mathbb{Z}$.

L'unicité découle de la proposition 1.17 ii) ■

Exercice 1.20 *Soit* $(a,b) \in \mathbb{N}^2$. *Montrer que* $H = \{ma+nb/\ m,n \in \mathbb{Z}\}$ *est le plus petit sous-groupe de* $\mathbb{Z}$ *contenant* $a\mathbb{Z} \cup b\mathbb{Z}$ *(*H *est appelé le sous groupe de* $\mathbb{Z}$ *engendré par* a *et* b *et se note* $H = a\mathbb{Z}+b\mathbb{Z}$*).*

1.3.3 PGCD et PPCM

Définitions et Propriétés

Théorème et Définition 1.21 *Soient* a *et* b *deux entiers relatifs non nuls. Alors,*

(i) Il existe un unique entier naturel non nul d *tel que :*

* d/a *et* d/b *et*

* *Si* $d' \in \mathbb{Z}$ *est tel que* d'/a *et* d'/b, *alors* d'/d *;* d *s'appelle le* ***plus grand diviseur commun*** *de* a *et* b *et se note* $\mathbf{d} = \mathbf{pgcd(a,b)}$, *ou simplement* $\mathbf{d} = \mathbf{a} \wedge \mathbf{b}$,

(ii) Il existe un unique entier naturel non nul m *tel que :*

* a/m *et* b/m *et*

* *Si* $m' \in \mathbb{Z}$ *est tel que* a/m' *et* b/m', *alors* m/m', m *s'appelle le* ***plus petit multiple commun*** *de* a *et* b *et se note* $\mathbf{m} = \mathbf{ppcm(a,b)}$, *ou simplement* $\mathbf{m} = \mathbf{a} \vee \mathbf{b}$

(iii) Deux entiers a *et* b *sont dits* ***premiers entre eux*** *si* $pgcd(a,b) = 1$.

Preuve. d (resp. m) est l'entier naturel tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ (resp. $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$) ■

Exercice 1.22 *Soient a,b et c des entiers relatifs non nuls. Montrer que*

1) $a \wedge (b \wedge c) = (a \wedge b) \wedge c$

2) $ab \wedge ac = |a| .(b \wedge c)$

3) $a \vee (b \vee c) = (a \vee b) \vee c$

4) $ab \vee ac = |a| .(b \vee c)$

Algorithme d'Euclide

Proposition 1.23 *Soient* a *et* b *deux entiers naturels non nuls tels que* $a = .bq+c$, *alors* $a \wedge b = b \wedge c$. *En particulier, si* r *est le reste de la division euclidienne de* a *par* b,*alors* $a \wedge b = b \wedge r$.

Preuve. $a = bq + c$ entraine que $c \in a\mathbb{Z} + b\mathbb{Z}$ et que $a \in b\mathbb{Z} + c\mathbb{Z}$. Ainsi, $b\mathbb{Z} + c\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$ et $a \wedge b = b \wedge c$ ■

Algorithme 1.24 (Algorithme d'Euclide) *Soient* a, b *deux entiers naturels non nuls tels que* $b < a$ *et* b *ne divise pas* a. *Alors,* $pgcd(a,b)$ *est le dernier reste non nul obtenu en appliquant l'algorithme d'Euclide. Cet' algorithme consiste à :*

* *Commencer par effectuer la division euclidienne de* a *par* b : $a = bq_1 + r_1$

* *Effectuer la division euclidienne de* b *par* r_1 : $b = r_1q_2 + r_2$

* *Effectuer la division euclidienne de* r_1 *par* r_2 : $r_1 = r_2q_3 + r_3$

...

La suite (r_i) *est telle que* $0 \leq r_{i+1} < r_i$. *Ainsi il existe nécessairement* n *tel que* $r_n \neq 0$ *et* $r_{n+1} = 0$. *D'autre part, d'après la proposition 1.23,* $a \wedge b = b \wedge r_1 = \ldots = r_{n-1} \wedge r_n = r_n$.

Exemple 1.25 *Considérons les entiers 1876 et 365. Alors,* $1876 = 365.5 + 51$, $365 = 51.7 + 8$, $51 = 8.6 + 3$, $8 = 3.2 + 2$ *et* $3 = 2.1 + 1$. *Ainsi, les entiers* 1876 *et* 365 *sont premiers entre-eux.*

Remarque 1.26

1) Si $p\gcd(a,b) = d$, *alors* $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$ *et ainsi,* $\exists u, v \in \mathbb{Z}$ *tels que* $au + bv = d$.

2) Une méthode pratique pour déterminer u *et* v *consiste à les calculer en remontant les égalités de l'algorithme d'Euclide.*

Exemple 1.27 *En considérant l'exemple précédent, on a :*
$1 = 3-2 = 3-(8-3.2) = 3(51-8.6)-8 = 3.51-8.19 = 3.51-19(365-51.7) = 136.51-19.365 = 136(1876-5.365)-19.365 = \mathbf{136}.1876 - \mathbf{699}.365.$

Méthode de Blankinship : Soient $(a,b) \in \mathbb{N}\times\mathbb{N}^*$: $a \geq b$. Vu que $a = 1.a+0.b$ et $b = 0.a+1.b$, on considère la matrice $A_0 = \begin{pmatrix} a & 1 & 0 \\ b & 0 & 1 \end{pmatrix}$. On passe de cette matrice à la deuxième matrice A_1 obtenue en remplaçant la première ligne L_1 de A_0 par $L_1 - q_1L_2$, où L_2 est la deuxième ligne de A_0 et q_1 est le quotient de la division euclidienne de a par b. Ainsi, la deuxième matrice obtenue est $A_1 = \begin{pmatrix} a-bq_1 = r_1 & 1 & -q_1 \\ b & 0 & 1 \end{pmatrix}$, où r_1 est le reste de la division euclidienne de a par b. Comme $b > r_1$, on obtient la troisième matrice en remplaçant la ligne L_2 par $L_2 - q_2L_1$, avec q_2 le quotient de la division euclidienne de b par r_1. La matrice obtenue est $A_2 = \begin{pmatrix} r_1 & 1 & -q_1 \\ b-q_2r_1 = r_2 & -q_2 & 1+q_1q_2 \end{pmatrix}$, etc.... Il est évident que le processus de détermination des matrices $A_i = \begin{pmatrix} r_i & x_i & y_i \\ r_{i+1} & x_{i+1} & y_{i+1} \end{pmatrix}$ n'est autre que l'algorithme d'Euclide avec $r_i = ax_i+by_i$ et $r_{i+1} = ax_{i+1}+by_{i+1}$ et donc si r_n est le dernier coefficient non nul de la suite (r_i), $r_n = a \wedge b$ et $r_n = ax_n + by_n$.

Exemple 1.28 *En reconsidérant l'exemple précédent* $a = 1876$ *et* $b = 365$*, on a la matrice* $\begin{pmatrix} 1876 & 1 & 0 \\ 365 & 0 & 1 \end{pmatrix}$*.*
Vu que $1876 = 365.5+51$*, on remplace* L_1 *par* $L_1 - 5.L_2$ *et par suite on obtient la matrice* $\begin{pmatrix} 51 & 1 & -5 \\ 365 & 0 & 1 \end{pmatrix}$*. Comme* $365 = 51.7+8$*, on remplace* L_2 *par* $L_2 - 7.L_1$ *et on obtient* $\begin{pmatrix} 51 & 1 & -5 \\ 8 & -7 & 36 \end{pmatrix}$*.*
On a $51 = 8.6+3$*, alors on remplace* L_1 *par* $L_1 - 6.L_2$ *et la matrice obtenue est* $\begin{pmatrix} 3 & 43 & -221 \\ 8 & -7 & 36 \end{pmatrix}$*.*
L'étape suivante consiste à remplacer L_2 *par* $L_2 - 2.L_1$ *(*$8 = 3.2+2$*) et on obtient* $\begin{pmatrix} 3 & 43 & -221 \\ 2 & -93 & 478 \end{pmatrix}$*.*
Puisque $3 = 2.1+1$*, on remplace* L_1 *par* $L_1 - L_2$ *et on obtient* $\begin{pmatrix} 1 & 136 & -669 \\ 2 & -93 & 478 \end{pmatrix}$*. Pour terminer, on a* $2 = 2.1$*, alors on remplace* L_2 *par* $L_2 - 2.L_1$ *et on obtient la matrice* $\begin{pmatrix} 1 & 136 & -669 \\ 0 & -365 & 1876 \end{pmatrix}$*.*
Ainsi, $1876 \wedge 365 = 1$ *et on a* $1 = 136.1876 - 669.365$*.*

Théorème 1.29 (Théorème de Bezout) *Soient a et b deux entiers naturels non nuls. Alors, a et b sont premiers entre eux si, et seulement si, il existe deux entiers relatifs u et v tels que $ua+vb = 1$.*

Preuve. D'après la remarque 1.26, si $p\gcd(a,b) = 1$, il existe $u, v \in \mathbb{Z}$: $ua+vb = 1$. Réciproquement, s'il existe u et v tels que $ua+vb = 1$, alors $a\mathbb{Z}+b\mathbb{Z} = \mathbb{Z}$ et ainsi $a \wedge b = 1$ ■

Exercice 1.30 *Soient a et b deux entiers naturels non nuls et d un diviseur commun de a et b. Montrer que $a \wedge b = d$ si, et seulement si, $\frac{a}{d} \wedge \frac{b}{d} = 1$.*

1.3.4 Nombres Premiers

Définition 1.31 *Soit p un entier naturel ≥ 2. On dit que p est un* ***nombre premier****, si 1 et p sont les seuls diviseurs de p dans $\mathbb{N}$, (i.e., Si $a \in \mathbb{N}$ et a/p alors $a = 1$ ou $a = p$).*
On désigne par $\mathcal{P}$ l'ensemble de tous les nombres premiers.

Exemple 1.32 $2, 3, 5, 7, 11, 2^{32582657}-1 \in \mathcal{P}$ *tandis que* $1, 4, 6, 8, 9, 2047 = 2^{11}-1 = 23.89 \notin \mathcal{P}$ *(site : www.utm.edu/research/primes/largest.html).*

Définition 1.33 *Un entier relatif n est dit premier si $|n|$ est un nombre premier, i.e., si $n \geq 2$ et les seuls diviseurs de n sont 1, -1, n et $-n$.*

Exercice 1.34 *Montrer que*

1) Si $a \in \mathbb{N}$ et p est un nombre premier, alors p/a ou $p \wedge a = 1$.

2) Si p et q sont deux entiers naturels premiers et distincts, alors $p \wedge q = 1$.

3) Montrer que tout entier $n \geq 2$, admet un diviseur premier (Ind : considérer l'ensemble $D = \{d \in \mathbb{N}/\ d \geq 2 \text{ et } d/n\}$, montrer que D possède un plus petit élément p et que p est premier).

Théorème 1.35 (Premier Théorème d'Euclide) *Soient p un nombre premier, a et b deux entiers. Si p divise ab, alors p divise a ou p divise b.*

Preuve. Supposons que $p \nmid a$, alors $p \wedge a = 1$ ((i) de l'exercice précédent), d'où $\exists\ u, v \in \mathbb{Z}$ tels que $ua + vp = 1$, ainsi $b = uab + vpb$ et puisque p/ab, alors p/b ■

Une conséquence de ce résultat est l'important théorème suivant :

Théorème 1.36 (Théorème fondamental de l'Arithmétique) *Tout entier naturel $n \geq 2$ admet une factorisation unique en nombres premiers, à l'ordre des facteurs près, i.e.,*

$\forall n \in \mathbb{N}^* - \{1\}$, $\exists! r \in \mathbb{N}^*$, $\exists!(p_1, \ldots, p_r) \in \mathcal{P}^r$, avec $p_1 < \ldots < p_r$, $n = p_1^{k_1} \ldots p_r^{k_r}$ et $k_1 \geq 1, \ldots, k_r \geq 1$.

Preuve. Existence : Appelons $P(n)$ la propriété « *n est un produit de nombres premiers* ». Puisque 2 est un nombre premier, 2 vérifie bien $P(n)$. Supposons $P(m)$ vraie pour tout entier $m < n$. Si n est premier, $P(n)$ est évidement vraie. Sinon, $n = ab$, avec $a < n$ et $b < n$. D'après l'hypothèse de récurrence, $P(a)$ et $P(b)$ sont vraies, i.e., a et b sont produits de nombres premiers, il en est de même de $n = ab$ et $P(n)$ est vraie $\forall n \geq 2$.

Unicité : Supposons que $n = p_1^{k_1} \ldots p_r^{k_r} = q_1^{l_1} \ldots q_s^{l_s}$ avec $p_1 < \ldots < p_r$ et $q_1 < \ldots < q_s$. Alors, p_1 divise $q_1^{l_1} \ldots q_s^{l_s}$ et en appliquant le théorème d'Euclide ($p/ab \ldots t$ alors p/a ou $p/b \ldots$ ou p/t), p_1 est égal à l'un des q_i, pour un certain i. Nécessairement $p_1 = q_1$ étant donné l'ordre imposé aux p_i et aux q_i respectivement. D'où, on déduit que $r = s$, $p_i = q_i$ et $k_i = l_i$ pour tout $i = 1, \ldots, r$ ■

Exemple 1.37 $368 = 2^4.23$, $369 = 3^2.41$, $370 = 2.5.37$, $371 = 53.7$, $372 = 2^2.3.31$ *et* 373 *est un nombre premier.*

Exercice 1.38 *Soit p un entier naturel ≥ 2 vérifiant la propriété suivante : $\forall a, b \in \mathbb{N}$, si p/ab, alors p/a ou p/b. Montrer que p est premier.*

Remarque 1.39 *Ecrivons $a = p_1^{k_1} \ldots p_r^{k_r}$ et $b = p_1^{l_1} \ldots p_r^{l_r}$ avec $k_1 \geq 0, \ldots, k_r \geq 0$ et $l_1 \geq 0, \ldots, l_r \geq 0$. Il est facile de voir que, si on pose $m(p_i) = min\{k_i, l_i\}$, $M(p_i) = max\{k_i, l_i\}$, alors $a \wedge b = p_1^{m(p_1)} \ldots p_r^{m(p_r)}$ et $a \vee b = p_1^{M(p_1)} \ldots p_r^{M(p_r)}$.*

Exemple 1.40 *On a $756 = 2^2.3^3.7$ et $240 = 2^4.3.5$, $pgcd(756, 240) = 2^2.3$ et $ppcm(756, 240) = 2^4.3^3.5.7$.*

Remarque 1.41 *Dans la pratique, il est difficile de savoir si un nombre donné est premier ou non et aussi de déterminer les nombres premiers qui figurent dans la décomposition d'un entier donné. Pour calculer le $pgcd(a, b)$ de deux entiers a et b, on applique plutôt l'algorithme d'Euclide.*

Lemme 1.42 (Lemme de Gauss) *Soient a, b et c des éléments de $\mathbb{Z}$. Si a/bc et $a \wedge b = 1$, alors a/c.*

Preuve. Il suffit pour démontrer ce résultat de considérer la décomposition de chacun des nombres a, b et c en nombres premiers et d'appliquer le théorème d'Euclide ■

Exercice 1.43 *En utilisant le théorème de Bezout, donner une autre démonstration du lemme de Gauss.*

Proposition 1.44 *Soient a,b et c des entiers naturels non nuls. Si $d = a \wedge b$ et $m = a \vee b$, alors $md = ab$. (En particulier, $d = 1$ si, et seulement si, $m = ab$).*

Preuve. Il suffit d'utiliser la remarque 1.39 ■

1.4 Congruences

Définition 1.45 *Soient $x, y \in \mathbb{Z}$ et $n \in \mathbb{N}$. On dit que* **x** ***est congru à*** **y** ***modulo*** **n** *et on écrit* $\mathbf{x} \equiv \mathbf{y} \pmod{\mathbf{n}}$ *(ou simplement $x \equiv y$), s'il existe $k \in \mathbb{Z}$ tel que $x - y = kn$, autrement dit si n divise $x - y$. On écrit aussi $x \not\equiv y \pmod n$ si x n'est pas congru à y modulo n.*

Exemple 1.46
1) Si $n = 1$, alors $\forall x, y \in \mathbb{Z}$, on a $x \equiv y$ (mod 1).
2) Si $n = 0$, alors $x \equiv y$ (mod 0) si, et seulement si, $x = y$.
3) $63 \equiv 39 \pmod 6$, $36 \equiv 64 \pmod{14}$ *mais* $16 \not\equiv 103 \pmod 2$.

Proposition 1.47 *Pour tout entier $n \in \mathbb{N}$,*
(i) La relation de congruence modulo n est une relation d'équivalence.
(ii) La relation de congruence modulo n est compatible avec l'addition (i,e. si $x \equiv y$ (mod n) et $x' \equiv y'$ (mod n) alors $x + x' \equiv y + y'$ (mod n)).
(iii) La relation de congruence modulo n est compatible avec la multiplication (i,e., si $x \equiv y$ (mod n) et $x' \equiv y'$ (mod n) alors $xx' \equiv yy'$ (mod n)).
(iv) Pour tout entier relatif x, il existe un, et un seul, entier r tel que $x \equiv r$ (mod n) et $0 \leq r < n$. L'entier r s'appelle ***le résidu de x modulo n*** *et ainsi deux entiers x et y ont le même résidu modulo n si, et seulement si, $x \equiv y$ (mod n).*

Preuve. Montrons par exemple (iii) : soient $x, x', y, y' \in \mathbb{Z} : x \equiv y \pmod n$ et $x' \equiv y'$ (mod n), alors $xx' - yy' = xx' - yx' + yx' - yy' = (x - y)x' + y(x' - y')$. Puisque $x \equiv y$ (mod n) et $x' \equiv y'$ (mod n), il existe $k, k' \in \mathbb{Z} : x - y = kn$ et $x' - y' = k'n$, alors $xx' - yy' = knx' + yk'n = (kx' + k'y)n$ et ainsi $xx' \equiv yy'$ (mod n).

La propriété (iv) découle du théorème de la division euclidienne (r est le reste de la division euclidienne de x par n) ■

Exemple 1.48 $63 = 6.10 + 3$, *ainsi* 3 *est le résidu de 63 modulo 6.*

La classe d'équivalence $\overline{x}$ de x modulo n est $\overline{x} = \{y \in \mathbb{Z}/\ y \equiv x \text{ (mod n)}\} = x + n\mathbb{Z}$ et toute classe possède un unique représentant compris entre 0 et $n - 1$. Ainsi $\overline{0} = n\mathbb{Z}, \ldots, \overline{n-1} = (n-1) + n\mathbb{Z}$ et l'ensemble, noté $\mathbb{Z}_n$ ou $\mathbb{Z}/n\mathbb{Z}$, des classes d'équivalence de la congruence modulo n est $\mathbb{Z}_n = \{\overline{0}, \ldots, \overline{n-1}\}$.

Les propriétés (ii) et (iii) de la proposition précédente montrent qu'on peut définir deux applications de $\mathbb{Z}_n \times \mathbb{Z}_n$ vers $\mathbb{Z}_n$ (i.e. deux lois de composition internes sur $\mathbb{Z}_n$) comme suit :

* La première loi est l'addition : $\forall \overline{x}, \overline{y} \in \mathbb{Z}_n$, $\overline{x} + \overline{y} := \overline{x + y}$
* La deuxième loi est la multiplication : $\forall \overline{x}, \overline{y} \in \mathbb{Z}_n$, $\overline{x}.\overline{y} := \overline{x.y}$.

On constate aisément que $\mathbb{Z}_n$, muni de cette addition, est un groupe abélien ; on a par exemple : $\overline{x}+\overline{0}=\overline{x}, \overline{x}+\overline{(-x)}=\overline{0}\dots$ i.e., $\overline{0}$ est l'élément neutre pour cette addition et le symétrique de $\overline{x}$ est $\overline{(-x)}$.

La multiplication est associative, commutative et distributive par rapport à l'addition ... et $(\mathbb{Z}_n, +, .)$ a une structure d'*anneau commutatif unitaire d'élément unité* $\overline{1}$.

Exercice 1.49 *Soit n>1.*

1) Montrer que $\mathcal{U}(\mathbb{Z}_n)=\{\overline{x}\in\mathbb{Z}_n/\exists\overline{y}\in\mathbb{Z}_n : \overline{x}.\overline{y}=\overline{1}\}$ *est un groupe pour la multiplication.*

2) Montre que $\overline{x}\in\mathcal{U}(\mathbb{Z}_n)$ *si, et seulement si,* $x\wedge n=1$.

3) $n=1876$. *Montrer que* $\overline{x}=\overline{365}\in\mathcal{U}(\mathbb{Z}_n)$ *et déterminer* $\overline{x}^{-1}$.

Chapitre 2

Groupes

2.1 Groupes

2.1.1 Définitions et Propriétés

Définition 2.1 *Soit G un ensemble non vide muni d'une loi de composition interne : une application* $g : G \times G \longrightarrow G$*, pour laquelle on note* $\forall x, y \in G$*,* $g(x, y) = x.y$ *ou* $x \top y, x \perp y, \ldots$ *ou simplement* xy.

On dit que $(G, .)$*, ou simplement* G*, est un* ***groupe*** *si :*

(i) la loi . est associative, i.e., $\forall x, y, z \in G, x.(y.z) = (x.y).z$,

(ii) la loi . possède un élément neutre, i.e., $\exists e \in G : \forall x \in G \; x.e = e.x = x$,

(iii) tout élément x *de* G *possède un symétrique* x'*, i.e.,* $\forall x \in G, \exists x' \in G : x.x' = x'.x = e$. *On désigne ce symétrique par* x^{-1} *et on l'appelle inverse de* x.

Si de plus la loi . est commutative, i.e., $\forall x, y \in G \; x.y = y.x$*, on dit que le groupe* G *est* ***commutatif*** *ou* ***abélien****. On note souvent dans ce cas la loi* $+$*, le neutre* 0*, le symétrique* $-x$ *et on l'appelle opposé de* x.

Exemple 2.2

1) $(\mathbb{R}, +), (\mathbb{Q}, +), (\mathbb{Z}, +)$ *sont des groupes abéliens.*

2) $(\mathbb{R}^*, .), (\mathbb{Q}^*, .)$*, ainsi que* $(\mathbb{R}^*_+, .), (\mathbb{Q}^*_+, .)$ *sont des groupes abéliens.*

3) L'ensemble $S(E)$ *des bijections d'un ensemble* E *non vide muni de la composition des applications :* $f \circ g : E \longrightarrow E$, $x \longmapsto f \circ g(x) = f(g(x))$ *est un groupe d'élément neutre* $Id_E : E \longrightarrow E, x \longmapsto x$ *appelée identité de* E*. Ce groupe n'est pas commutatif dès que* $card(E) \geq 3$*. En effet, soient* x, y, z *trois éléments de* E *deux à deux différents et soient* f *et* g *les deux applications définies par :* $f(x) = y, f(y) = z, f(z) = x, f(t) = t$ *si* $t \neq x, t \neq y, t \neq z$ *et* $g(x) = x, g(y) = z, g(z) = y$ *et* $g(t) = t$ *si* $t \neq x, t \neq y, t \neq z$*. Alors,* f *et* g *sont des bijections et* $f \circ g(x) = f(g(x)) = f(x) = y$ *et* $g \circ f(x) = g(f(x)) = g(y) = z$*. Ainsi* $f \circ g \neq g \circ f$.

4) $(\mathcal{M}_{n,p}(\mathbb{R}), +)$ *est un groupe abélien.*

5) Soit n *un entier naturel,* $n \notin \{0, 1\}$*. Alors, l'ensemble* $(GL_n(\mathbb{R}), .)$ *des matrices carrées inversibles d'ordre* n *à coefficients dans* $\mathbb{R}$*, muni du produit des matrices, est un groupe non abélien appelé* ***groupe linéaire****.*

6) $(\mathbb{Z}_n, +)$ *est un groupe commutatif.*

Proposition 2.3 *Soit* G *un groupe noté multiplicativement. Alors,*

(i) L'élément neutre de G *est unique, aussi le symétrique de tout élément* a *de* G *est unique.*

(ii) $\forall a \in G, \forall m, n \in \mathbb{Z} : a^m a^n = a^{m+n}$.

(iii) tout élément a *de* G *est régulier, plus précisément :* $\forall a, b \in G$*, l'équation* $ax = b$ *(resp.* $xa = b$*) possède une unique solution qui est* $x = a^{-1}b$ *(resp.* $x = ba^{-1}$*).*

*(iv) Si G et G' sont deux groupes, $G \times G'$ est muni d'une structure de groupe en posant : $\forall (a,b),(c,d) \in G \times G'$: $(a,b)(c,d) = (ac, bd)$. $G \times G'$ muni de cette loi est appelé **groupe produit** (des groupes G et G').*

Preuve. Montrons par exemple la propriété (i) : Si e et e' sont neutres, $e' = ee' = e$. De même, si x' et x" sont des symétriques de x , alors $x' = x'e = x'(xx") = (x'x)x" = ex" = x"$ ■

2.1.2 Sous-groupes

Définition 2.4 *Soit $(G, .)$ un groupe et H une partie de G. On dit que H est un **sous-groupe** de G si :*

(i) H est stable, i.e., $\forall x, y \in H$, $x.y \in H$, autrement dit la restriction de la loi . à H est une loi de composition interne

(ii) $(H, .)$ est un groupe.

Proposition 2.5 *Soit G un groupe et H une partie de G. Alors, on a l'équivalence des trois propositions suivantes :*

(i) H est un sous-groupe de G

(ii) $H \neq \emptyset$, $\forall x, y \in H, x.y \in H$ et $\forall x \in H, x^{-1} \in H$

(iii) $H \neq \emptyset$ et $\forall x, y \in H$, $x.y^{-1} \in H$

Preuve. Par définition (i) entraine (ii) et (ii) implique aussi (iii) car $\forall x, y \in H$, on a $y^{-1} \in H$ et $xy^{-1} \in H$.

Montrons que (iii) entraine (i) : considérons $x \in H$ ($H \neq \emptyset$), alors $e = xx^{-1} \in H$. De même, $\forall x \in H : x^{-1} = ex^{-1} \in H$ et on a $\forall x, y \in H : xy = x((y)^{-1})^{-1} \in H$. L'associativité de . dans H découle de l'associativité de . dans G ■

Exemple 2.6

1) $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Q}, +)$ et $(\mathbb{Q}, +)$ est un sous- groupe de $(\mathbb{R}, +)$.

2) $(\{-1, 1\}, .)$ est un sous-groupe de $(\mathbb{Q}^*, .)$ qui lui même est un sous-groupe de $(\mathbb{R}^*, .)$.

*3) Si G est un groupe, alors $\{e\}$ et G sont des sous-groupes de G appelés **sous-groupes triviaux** de G.*

4) Si H et K sont des sous groupes de G, alors $H \cap K$ est un sous-groupe de G. En général si I est un ensemble d'indices et $(H_i)_{i \in I}$ une famille de sous-groupes de G, alors $\bigcap_{i \in I} H_i$ est un sous-groupe de G.

5) Les sous-groupes de $\mathbb{Z}$ sont tous de la forme $n\mathbb{Z}$, avec $n \in \mathbb{N}$ (cf. Chapitre I).

6) $SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) / \ det(A) = 1\}$ est un sous-groupe de $GL_n(\mathbb{R})$.

7) L'ensemble $R(P)$ des rotations du plan P muni de la composition des applications est un sous-groupe de $S(P)$. En effet, si r_θ (resp. $r_{\theta'}$) est une rotation d'angle θ (resp. θ'), alors $r_\theta \circ r_{\theta'} = r_{\theta+\theta'}$ et ainsi $r_\theta \circ r_{\theta'}^{-1} = r_{\theta-\theta'} \in R(P)\ldots$

8) Si H et K sont deux sous-groupes de G, alors, en général, $H \cup K$ n'est pas un sous-groupe de G. Soient, par exemple, $H = \{(x, y) \in \mathbb{R}^2 / \ x = 0\}$ et $K = \{(x, y) \in \mathbb{R}^2 / \ y = 0\}$. Il est évident que H et K sont deux sous-groupes du groupe additif $\mathbb{R}^2$. Cependant, $H \cup K$ n'est pas un sous-groupe de $\mathbb{R}^2$ car on a par exemple $(0, 1) + (1, 0) = (1, 1) \notin H \cup K$.

Exercice 2.7 *Soient H et K deux sous-groupes d'un groupe G. Montrer que $H \cup K$ est un sous-groupe de G si, et seulement si, $H \subset K$ ou $K \subset H$.*

Exercice 2.8 *Soient G un groupe noté multiplicativement, H et K deux sous-groupes de G. Montrer que $HK = \{x \in G / \ \exists h \in H, \exists k \in K : x = hk\}$ est un sous-groupe de G si, et seulement si, $HK = KH$.*

2.1.3 Homomorphismes de groupes

Soient G et G' deux groupes et $f : G \longrightarrow G'$ une application de G vers G'.

Définition 2.9 *On dit que f est un* ***homomorphisme de groupes****, ou* ***morphisme de groupes****, si pour tous x, y éléments de G : $f(xy) = f(x)f(y)$.*

Si de plus f est bijective, f est appelé un ***isomorphisme de groupes****. Si $G = G'$, on dit que f est un* ***endomorphisme*** *de G et si en outre f est une bijection, on dit alors que f est un* ***automorphisme*** *de G.*

Exemple 2.10

1) Soient G, G' deux groupes et e' l'élément neutre de G'. L'application $f : G \longrightarrow G', x \longmapsto e'$ est un homomorphisme de groupes.

2) Soit G un groupe, $a \in G$. Alors l'application $\tau_a : G \longrightarrow G$, $x \longmapsto axa^{-1}$ est un automorphisme de G appelé ***automorphisme intérieur****. On a $\tau_e = Id_G$ et si G est commutatif, $\tau_a = Id_G$ $\forall a \in G$.*

3) Soit G un groupe noté multiplicativement. L'application $\varphi : \mathbb{Z} \longrightarrow G$, $n \longmapsto a^n$ est un homomorphisme de groupes.

4) Soit $f : \mathbb{R} \longrightarrow R(P)$, $\theta \longmapsto r_\theta$. f est bien un homomorphisme de groupes puisque $r_\theta \circ r_{\theta'} = r_{\theta+\theta'}$.

Propriétés 2.11 *Soient G, G' deux groupes d'éléments neutres respectifs e et e' et $f : G \longrightarrow G'$ un homomorphisme de groupes. Alors,*

(i) $f(e) = e'$ et $\forall x \in G$, $f(x^{-1}) = (f(x))^{-1}$.

(ii) Pour tout sous-groupe H de G, l'ensemble $f(H) = \{f(x)/\ x \in H\}$ est un sous-groupe de G'. En particulier, $\operatorname{Im} f = f(G)$ est un sous-groupe de G'.

(iii) Pour tout sous-groupe H' de G', $f^{-1}(H') = \{x \in G/\ f(x) \in H'\}$ est un sous-groupe de G. En particulier, $f^{-1}(\{e'\}) = \{x \in G/\ f(x) = e'\}$ est un sous-groupe de G noté $\ker f$ est appelé ***noyau de f****.*

(iv) f est injective si ,et seulement si, $\ker f = \{e\}$.

(v) Soient $G, G', G"$ trois groupes, $f : G \longrightarrow G'$ et $g : G' \longrightarrow G"$ deux homomorphismes de groupes. Alors $g \circ f$ est un homomorphisme de groupes.

(vi) Si f est un isomorphisme alors f^{-1} est aussi un isomorphisme de groupes. De sorte que si on note $Aut(G)$ l'ensemble de tous les automorphismes de G, alors $(Aut(G), \circ)$ est un groupe.

2.1.4 Groupes monogènes, Groupes cycliques

Définition et Proposition 2.12 *Soit X une partie d'un groupe G. On appelle* ***sous-groupe engendré par*** *X et on note $< X >$ l'intersection de tous les sous-groupes de G contenant X.*

$< X >$ est le plus petit sous-groupe de G contenant X.

Si H est un sous-groupe de G et si $H =< X >$, on dit que H ***est engendré par*** *X.*

Remarque 2.13 *Si H est un sous-groupe de G, on a toujours $H =< H >$, mais les parties génératrices intéressantes sont celles qui ont le moins d'éléments possibles.*

Proposition 2.14 *Soit X une partie non vide d'un groupe G noté multiplicativement. Alors $< X >= \{a_1a_2...a_n/\ n \in \mathbb{N}$ et $\forall i = 1, \ldots, n : a_i \in X$ ou $a_i \in X^{-1}\}$.*

Preuve. Notons H l'ensemble de ces produits. Alors, la proposition 2.5 entraîne que H est bien un sous-groupe de G. Soit maintenant K un autre sous-groupe de G contenant X. On a d'abord, $\forall a \in X, a \in K$ et $a^{-1} \in K$ et puisque K est stable, tous les produits de la forme $a_1a_2...a_n$, $n \in \mathbb{N}^*$, $a_i \in X$ ou $a_i \in X^{-1}$, appartiennent à K et ainsi $H \subset K$ ∎

Exemple 2.15

1) Si $X = \emptyset$, alors $< X >= \{e\}$.

2) Si $X = \{a\}$, alors $< a >= \{a^n / \ n \in \mathbb{Z}\} = \varphi(\mathbb{Z})$, où φ est le morphisme 3) de l'exemple 2.10.

Exercice 2.16 *Soient H et K deux sous-groupes de G tels que $HK = KH$. Vérifier que $HK =< H \cup K >$.*

Définition 2.17 *Un groupe G est dit **monogène** s'il existe un élément a de G tel que G est engendré par a, i.e., $G =< a >$.*

*Si $G =< a >$ et si de plus G est fini, on dit que G est **cyclique** engendré par a.*

Exemple 2.18

1) Tout sous-groupe de $\mathbb{Z}$ est monogène : $\{0\} =< 0 >, \mathbb{Z} =< 1 >$ et si H est un sous-groupe non trivial de $\mathbb{Z}$, n le plus petit entier positif non nul appartenant à H, on a $H =< n >= n\mathbb{Z}$ (cf. chapitre I, Théorème 1.19).

2) $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ est un groupe cyclique d'ordre n engendré par $\bar{1}$: $\bar{0} = 0.\bar{1}$, $\bar{1} = 1.\bar{1}$, $\bar{2} = \bar{1} + \bar{1} = 2.\bar{1}, \dots, \overline{n-1} = (n-1).\bar{1}$.

Définition 2.19 *Soient G un groupe et n un entier ≥ 1. Si $|G| = n$, on dit que G est un **groupe fini d'ordre n**. On dit aussi qu'un sous-groupe H de G est d'ordre d si H est fini et $|H| = d$. On écrit alors $\mathbf{o(G) = n}$, $\mathbf{o(H) = d}$.*

*Un **élément** a de G est dit **d'ordre fini** égal à d et on note $\mathbf{o(a) = d}$, si le sous-groupe $< a >$ de G engendré par a est fini d'ordre d .*

Exemple 2.20

1) Tous les éléments d'un groupe fini sont d'ordres finis. En particulier dans $\mathbb{Z}_n$, tout élément est d'ordre fini, on a par exemple : $o(\bar{1}) = o(\mathbb{Z}_n) = n$.

2) Dans $\mathbb{Z} \times \mathbb{Z}_n$, l'élément $(1, \bar{0})$ n'est pas d'ordre fini alors que $(0, \bar{1})$ est d'ordre fini égal à n.

Proposition 2.21

(i) Soient G un groupe, a un élément de G et d un entier naturel non nul. Si a est d'ordre d, alors $< a >= \{a^n / \ 0 \leq n \leq d-1\} = \{e, a, ..., a^{d-1}\}$.

(ii) Si $G =< a >\neq \{e\}$ et H est un sous-groupe de G différent de $\{e\}$, alors $H =< a^m >$ où m est le plus petit entier strictement positif tel que $a^m \in H$.

Preuve. (i) Soit d' le plus petit entier strictement positif tel que $a^{d'} = e$ (un tel entier existe car $< a >$ est fini). Alors, pour tout entier $m \in \mathbb{Z}$, il existe $(q, r) \in \mathbb{Z}^2$: $m = qd' + r$ avec $0 \leq r < d'$. Ainsi, $a^m = a^{qd'+r} = (a^{d'})^q a^r = ea^r = a^r$ et alors $< a >\subset \{e, a, ..., a^{d'-1}\}$ et puisque $\{e, a, ..., a^{d'-1}\} \subset< a >$, on a $< a >= \{e, a, ..., a^{d'-1}\}$ et $d' = d$ (car les éléments $e, a, ..., a^{d'-1}$ sont deux à deux distincts).

(ii) Puisque H est un sous-groupe de G différent de $\{e\}$, il existe un plus plus petit entier strictement positif m tel que $a^m \in H$ et alors, $< a^m >\subset H$. D'autre part, si $x \in H$, alors $\exists l \in \mathbb{Z} : x = a^l$ (car $H \subset G =< a >$). En effectuant la division euclidienne de l par m, $\exists!(q, r) \in \mathbb{Z}^2 : l = qm + r$ avec $0 \leq r < m$ ainsi $a^r = a^{l-qm} = a^l(a^m)^{-q} \in H$ et alors $r = 0$ (car m est le plus petit entier strictement positif tel que $a^m \in H$) et ceci prouve que $x = a^l = (a^m)^q \in< a^m >$ ■

Remarque 2.22

1) Si a un élément de G d'ordre d, alors d est le plus petit entier strictement positif vérifiant $a^d = e$. En effet, d'après la preuve de i) de la proposition précédente, on a $d(= d')$ est le plus petit entier strictement positif tel que $a^d = e$.

2) Soit a un élément de G d'ordre d et k un entier non nul. Si $a^k = e$ alors d divise k. En effet, effectuons la division euclidienne de k par d : $\exists!(q,r) \in \mathbb{Z}^2 : k = dq + r$ *avec* $0 \leq r < d$. *Ainsi* $e = a^k = a^{dq+r} = (a^d)^q a^r = ea^r$ *(car $a^d = e$) et alors $e = a^r$. Or r vérifie $0 \leq r < d$ et, d'après la remarque précédente, d est le plus petit entier strictement positif vérifiant $a^d = e$ et ceci prouve que $r = 0$, i.e., d divise k.*

Exercice 2.23 *Soient G un groupe, d un entier naturel non nul, a un élément de G et φ l'homomorphisme de groupes* $\varphi : \mathbb{Z} \longrightarrow G$, $n \longmapsto a^n$. *Alors $o(a) = d$ si, et seulement si, $ker\varphi = d\mathbb{Z}$.*

Exercice 2.24 *Soit G un groupe monogène. Montrer que*
1) Si G est infini, alors $G \simeq \mathbb{Z}$
2) Si G est fini d'ordre n, alors $G \simeq \mathbb{Z}_n$.

Exercice 2.25 *Soit $\bar{m} \in \mathbb{Z}_n$. Montrer que $\mathbb{Z}_n =< \bar{m} >$ si, et seulemnt si, $m \wedge n = 1$.*

2.2 Groupes quotients

2.2.1 Classes modulo un sous-groupe

Théorème et Définition 2.26 *Soient G un groupe et H un sous-groupe de G. Alors,*
(i) Les deux relations binaires suivantes :
(a) $\forall x, y \in G$, $x\mathcal{R}_g y$ si, et seulement si, $x^{-1}y \in H$
(b) $\forall x, y \in G$, $x\mathcal{R}_d y$ si, et seulement si, $xy^{-1} \in H$
sont des relations d'équivalence sur G.
(ii) La classe $\bar{x}_g$ de x modulo $\mathcal{R}_g$ (resp. modulo $\mathcal{R}_d$), appelée ***classe de** x **modulo** H **à gauche*** *(resp.* ***classe de** x **modulo** H **à droite***) *est l'ensemble $xH = \{xh/\ h \in H\}$ (resp. $Hx = \{hx/\ h \in H\}$. En particulier, $\bar{e}_g = \bar{e}_d = H$. On note $(\mathbf{G/H})_g$ (resp. $(\mathbf{G/H})_d$) l'ensemble des classes modulo $\mathcal{R}_g$ (resp. modulo $\mathcal{R}_d$).*
(iii) La translation $\tau : H \longrightarrow \bar{x}_g = xH$ (resp. $\tau' : H \longrightarrow \bar{x}_d = Hx$), $h \longmapsto xh$ (resp. $h \longmapsto hx$) est une bijection.
(iv) La correspondance définie de $(G/H)_g$ vers $(G/H)_d$ par : $xH \longmapsto Hx$ est une bijection. En particulier, $(G/H)_g$ et $(G/H)_d$ ont même cardinal.

Exemple 2.27
1) Si $H = G$, alors $\mathcal{R}_g$ et $\mathcal{R}_d$ sont des relations triviales, i.e., $\forall x, y \in G : x\mathcal{R}_g y$ et $x\mathcal{R}_d y$ et ainsi $(\mathbf{G/H})_g = (\mathbf{G/H})_d = \{G\}$.
2) Si $H = \{e\}$, alors deux éléments x et y de G ne sont en relation modulo H à gauche (resp. modulo H à droite) que si $x = y$ et ainsi $(\mathbf{G/H})_g = (\mathbf{G/H})_d = \{\{x\}/\ x \in G\}$.
3) On considère $G = GL_2(\mathbb{R})$, $H = SL_2(\mathbb{R})$ et $A, B \in GL_2(\mathbb{R})$. Alors, $A\mathcal{R}_g B$ si $A^{-1}B \in H$, i.e., $det(A) = det(B)$, ce qui revient à dire que $det(AB^{-1}) = 1$. Ainsi, dans cet exemple, les classes à droite modulo H et les classes à gauche modulo H sont identiques.
L'ensemble $\{\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} /\ a \in \mathbb{R}^*\}$ *est un ensemble de représentants des classes qui est par conséquent en bijection avec $\mathbb{R}^*$.*

Remarque 2.28
1) Si le groupe G est commutatif, alors $\mathcal{R}_g = \mathcal{R}_d$. En effet, $x\mathcal{R}_g y$ si, et seulement si, $x^{-1}y \in H$ si,et seulement si, $yx^{-1} \in H$ si, et seulement si, $(yx^{-1})^{-1} = xy^{-1} \in H$ si, et seulement si, $x\mathcal{R}_d y$.
2) Les classes modulo H à gauche (resp. modulo H à droite) forment une partition de G, i.e.,
(i) $\forall x \in G$, $xH \neq \emptyset$ (resp. $Hx \neq \emptyset$)

(ii) $\forall x, y \in G$, $xH \neq yH$ *(resp.* $Hx \neq Hy$*) si, et seulement si,* $xH \cap yH = \emptyset$ *(resp.* $Hx \cap Hy = \emptyset$*)*
(iii) $G = \bigcup_{x \in G} xH$ *(resp.* $G = \bigcup_{x \in G} Hx$*).*

Définition 2.29 *Soient* G *un groupe et* H *un sous-groupe de* G*. On note* $[\mathbf{G} : \mathbf{H}]$ *le cardinal* $|(G/H)_g| = |(G/H)_d|$ *et on l'appelle* ***indice de H dans G****.*

Théorème 2.30 (Théorème de Lagrange) *Soient* G *un groupe fini et* H *un sous-groupe de* G*. Alors,* $|G| = [G : H].|H|$*.*

Preuve. D'après le théorème et définition 2.26, les classes à gauche (resp. à droite) ont le même nombre d'éléments : à savoir $|H|$, et comme les classes d'équivalences forment une partition de G, $|G| = [G : H]\,|H|$ ■

Conséquence 2.31 *Si* G *est un groupe fini, alors l'ordre de tout sous-groupe* H *de* G *divise l'ordre de* G*. En particulier, l'ordre* $o(a)$ *de tout élément* a *de* G *divise l'ordre de* G*.*

Corollaire 2.32
(i) Si G *est un groupe fini d'ordre* n*, alors* $\forall a \in G$, $a^n = e$*.*
(ii) Si p *est un nombre premier et* G *un groupe d'ordre* p*, alors* G *est cyclique engendré par l'un quelconque de ses éléments différents de* e*.*

Preuve. (i) Si $o(a) = d$, alors d/n donc il existe $k \in \mathbb{N} : n = dk$ et ainsi $a^n = (a^d)^k = e^k = e$.
(ii) Soit $a \in G$, $a \neq e$, alors $o(a)/p$ et $o(a) \neq 1$, ainsi $o(a) = p$ et $G = \langle a \rangle$ ■

Conséquence 2.33 (Petit Théorème de Fermat) *Soit* p *un nombre premier. Alors, pour tout entier* a *non divisible par* p*, on a* $a^{p-1} \equiv 1 \pmod p$*.*

Preuve. $(\mathbb{Z}/p\mathbb{Z})^*$ est un groupe multiplicatif d'ordre $p-1$ et ainsi $\forall \bar{a} \in (\mathbb{Z}/p\mathbb{Z})^*, (\bar{a})^{p-1} = \bar{1}$ ■

Exercice 2.34 (Formule des indices) *Soient* G *un groupe,* H *et* K *deux sous-groupes de* G *tels que* $K \subset H$*. Montrer que* $[G : K] = [G : H].[H : K]$*.*

2.2.2 Sous-groupes distingués

Proposition et Définition 2.35 *Soient* G *un groupe et* H *un sous-groupe de* G*. Les propositions suivantes sont équivalentes :*
(i) Pour tout x *élément de* G *:* $xHx^{-1} \subset H$
(ii) Pour tout x *élément de* G *:* $xHx^{-1} = H$
(iii) Pour tout x *élément de* G *:* $xH = Hx$
Un sous-groupe H *de* G *vérifiant l'une de ces propriétés équivalentes est appelé sous-groupe* ***distingué*** *(ou* ***normal*** *ou* ***invariant****) du groupe* G *et on note* $H \lhd G$*.*

Exemple 2.36
1) Si G *est un groupe, alors* G *et* $\{e\}$ *sont des sous-groupes distingués de* G*.*
2) Si G *est un groupe commutatif, alors tout sous-groupe de* G *est un sous-groupe distingué de* G*.*
3) L'ensemble $\{z \in G / \ \forall x \in G : zx = xz\}$ *, noté* $Z(G)$*, est un sous-groupe distingué de* G *appelé* ***centre de G****.*
4) Tout sous-groupe H *d'indice* 2 *dans un groupe* G *est distingué. En effet, soit* $x \notin H$*, alors* $(G/H)_g = \{H, xH\}$ *et* $(G/H)_d = \{H, Hx\}$ *et ainsi* $xH = G - H = Hx$*.*
5) Dans $GL_n(\mathbb{R})$*, le sous-groupe* $SL_n(\mathbb{R})$ *est distingué puisque si* $B \in SL_n(\mathbb{R})$*,* $A \in GL_n(\mathbb{R})$*, alors* $det(ABA^{-1}) = (detA)(detB)(detA)^{-1} = detB = 1$*.*

2.2.3 Groupes quotients

Soient G un groupe et H un sous-groupe distingué de G. Alors $\mathcal{R}_g = \mathcal{R}_d$, pour tout x élément de G, $\bar{x}_g = xH = Hx = \bar{x}_d$ et on note $\bar{x} = \bar{x}_g = \bar{x}_d$ et $\overline{G/H} = (G/H)_g = (G/H)_d$.

La relation $\mathcal{R}$ ($\mathcal{R} = \mathcal{R}_g = \mathcal{R}_d$) est compatible avec la loi du groupe, i.e., $\forall a, b, a', b' \in G$: Si $\begin{cases} a\mathcal{R}a' \\ b\mathcal{R}b' \end{cases}$, alors $ab\mathcal{R}a'b'$. En effet, on a $a^{-1}a' \in H$ et $b^{-1}b' \in H$, ainsi $(ab)^{-1}(a'b') = b^{-1}a^{-1}a'b' = (b^{-1}(a^{-1}a')b)b^{-1}b' \in H$ car $a^{-1}a' \in H$ et $H \lhd G$.

Dans ce cas, la correspondance $(G/H) \times (G/H) \longrightarrow (G/H), (\bar{x}, \bar{y}) \longmapsto \bar{x}.\bar{y} = \overline{xy}$ est une application bien définie et constitue ainsi une loi de composition interne sur G/H.

Théorème et Définition 2.37 *Soient G un groupe et H un sous-groupe distingué de G. La relation binaire sur G définie par $x\mathcal{R}y$ si, et seulement si, $x^{-1}y \in H$ est une relation d'équivalence sur G compatible avec la loi du groupe et appelée* ***relation de congruence modulo*** *H.*

L'ensemble quotient, noté G/H, muni de la loi $\bar{x}, \bar{y} \in G/H$, $\bar{x}.\bar{y} = \overline{xy}$, est un groupe appelé ***groupe quotient de G par H*** *et la* ***surjection canonique*** *$s : G \longrightarrow G/H$, $x \longmapsto \bar{x}$ est un homomorphisme de groupes (on écrit dans ce cas, $x \equiv y \pmod H$ pour désigner que $x\mathcal{R}y$).*

Preuve. La loi est bien définie (voir ci-dessus) et est associative : $\forall x, y, z \in G$: $\bar{x}(\overline{\bar{y}\bar{z}}) = \overline{x(yz)} = \overline{(xy)z} = \overline{(\bar{x}\bar{y})}\bar{z}$. Aussi, on a $\bar{e} = H$ est neutre pour cette loi et $\forall x \in G$: $(\bar{x})^{-1} = \overline{x^{-1}}$ (en effet, $\bar{x}\overline{x^{-1}} = \overline{xx^{-1}} = \bar{e}$ et aussi $\overline{x^{-1}}\bar{x} = \bar{e}$). Enfin, la surjection canonique $s : G \longrightarrow G/H$, $x \longmapsto \bar{x}$ est un homomorphisme de groupes par définition de la loi dans G/H ■

Exemple 2.38 *On considère $G = \mathbb{Z}$ et $H = n\mathbb{Z}$ avec $n \in \mathbb{N}$. Puisque $\mathbb{Z}$ est commutatif, le sous-groupe $n\mathbb{Z}$ est distingué dans $\mathbb{Z}$. Deux entiers x et y sont en relation modulo $n\mathbb{Z}$ si, et seulement si, $x - y \in n\mathbb{Z}$, si, et seulement si, $n/x - y$ (ou $\exists k \in \mathbb{Z} : x - y = nk$) i.e., $x \equiv y \pmod n$ (cf. chapitre I, congruences) et ainsi la notation $\mathbb{Z}_n = G/H = \mathbb{Z}/n\mathbb{Z}$ est justifiée.*

Proposition 2.39 *Soit G, G' deux groupes et $f : G \longrightarrow G'$ un homomorphisme de groupes. Alors, $\ker f$ est un sous-groupe distingué de G. De plus, $x \equiv y \pmod{\ker f}$ si, et seulement si, $f(x) = f(y)$.*

Preuve. $\forall x \in G, \forall y \in \ker f$, $f(xyx^{-1}) = f(x)f(y)f(x^{-1}) = f(x)e'f(x^{-1}) = f(xx^{-1}) = e'$. D'autre part, on a $x \equiv y \pmod{\ker f}$ si, et seulement si, $x^{-1}y \in \ker f$, si, et seulement si, $f(x^{-1}y) = e'$ si, et seulement si, $f(x) = f(y)$ ■

2.3 Théorèmes d'isomorphisme

Théorème 2.40 (Premier théorème d'isomorphisme) *Soit $f : G \longrightarrow G'$ un homomorphisme de groupes. Alors, les groupes $G/Ker(f)$ et $Im(f)$ sont isomorphes ($G/\ker f \simeq Imf$).*

Preuve. Considérons $\bar{f} : G/Ker(f) \longrightarrow f(G), \bar{x} \longmapsto \bar{f}(\bar{x}) = f(x)$. $\bar{f}$ est une application bien définie d'après la proposition précédente. Aussi, $\operatorname{Im} \bar{f} = Imf$. D'autre part, $\bar{f}$ est un homomorphisme de groupes. En effet, $\bar{f}(\overline{\bar{x}\bar{x'}}) == \bar{f}(\overline{xx'}) = f(xx') = f(x)f(x') = \bar{f}(\bar{x})\bar{f}(\overline{x'})$. $\bar{f}$ est injectif car si $x \in G$: $\bar{f}(\bar{x}) = e'$, alors $f(x) = e'$ d'où $x \in \ker f$, i.e., $\bar{x} = \bar{e}$ et aussi $\bar{f}$ est par définition surjectif. Ainsi $G/\ker f \simeq Imf$ ■

Exemple 2.41 *L'application $f : \mathbb{R}^* \longrightarrow \mathbb{R}^*, x \longmapsto |x|$ est un homomorphisme des groupes. Alors, puisque $\ker f = \{-1, 1\}$ et $\operatorname{Im} f = \mathbb{R}^*_+$, $\mathbb{R}^*/\{-1, 1\} \simeq \mathbb{R}^*_+$.*

Théorème 2.42 (Deuxième théorème d'isomorphisme) *Soient G un groupe, H et K deux sous-groupes de G avec H distingué dans G. Alors,*

(i) $H \cap K$ est un sous-groupe distingué de K

(ii) HK est un sous-groupe de G

(iii) Les deux groupes HK/H et $K/H \cap K$ sont isomorphes.

Preuve. (ii) Il est facile de vérifier que $HK = KH$ (si $x \in KH$, alors $\exists h \in H, \exists k \in K : x = kh$ et puisque $kH = Hk$, il existe $h' \in H$ tel que $x = kh = h'k$ et alors $x \in HK$) et ainsi HK est un sous-groupe de G d'après l'exercice 2.8.

(i) et (iii) Soit $s : G \longrightarrow G/H$ la surjection canonique et $s_K : K \longrightarrow G/H$ la restriction de s à K. On a $\ker s_K = H \cap K$ et ainsi, d'après la proposition 2.39, $H \cap K$ est un sous-groupe distingué de K. D'autre part, d'après le premier théorème d'isomorphisme appliqué à s_K, $K/H \cap K \simeq \operatorname{Im} s_K$. Mais, $\operatorname{Im} s_K = \{kH/\ k \in K\} = HK/H$ et ainsi $HK/H \simeq K/H \cap K$ ■

Exemple 2.43 *Considérons le groupe additif $G = \mathbb{Z}$, $H = 9\mathbb{Z}$ et $K = 12\mathbb{Z}$. Alors, $H + K = 3\mathbb{Z}$, $H \cap K = 36\mathbb{Z}$ et ainsi $(3\mathbb{Z})/(9\mathbb{Z}) \simeq (12\mathbb{Z})/(36\mathbb{Z})$.*

Théorème 2.44 (Troisième théorème d'isomorphisme) *Soient H et K deux sous-groupes distingués d'un groupe G tels que $H \subset K$. Alors,*

(i) K/H est un sous-groupe distingué de G/H

(ii) les deux groupes G/K et $(G/H)/(K/H)$ sont isomorphes, i.e : $G/K \simeq (G/H)/(K/H)$

Preuve. Soit $f : G/H \longrightarrow G/K$, définie par : $f(xH) = xK$.

En utilisant le fait que $H \subset K$, on peut vérifier que f est une application bien définie. Aussi f est un homomorphisme de groupes surjectif. Déterminons son noyau : $\ker f = \{xH/\ xK = K\} = \{xH/\ x \in K\} = K/H$ et ainsi $\ker f = K/H \lhd G/H$ et, d'après le premier théorème d'isomorphisme, on a bien : $G/K \simeq (G/H)/(K/H)$ ■

Théorème 2.45 (Théorème de correspondance) *Soient G un groupe, H un sous-groupe distingué de G et $s : G \longrightarrow G/H$ la surjection canonique. Alors, L'application $K \longmapsto K/H$ définie une correspondance biunivoque entre les sous-groupes (resp. sous-groupes distingués) de G contenant H et les sous-groupes (resp. sous-groupes distingués) de G/H, i.e., T est un sous-groupe (resp. sous groupe distingué) de G/H si, et seulement si, il existe un sous-groupe (resp. sous-groupe distingué) K de G contenant H tel que $T = K/H$.*

De plus, si K_1 et K_2 sont deux sous-groupes de G contenant H alors $K_1 \subset K_2$ si, et seulement si, $K_1/H \subset K_2/H$ et dans ce cas $[K_2 : K_1] = [K_2/H : K_1/H]$.

Preuve. Soit $\varphi : \{K/\ K$ est un sous-groupe de G contenant $H\} \longrightarrow \{T/\ T$ est un sous-groupe de $G/H\}$ définie par : $\varphi(K) = K/H$.

Si K est un sous-groupe de G contenant H, alors il est clair, puisque s est un homomorphisme de groupes, que $s(K) = K/H = \varphi(K)$ est un sous-groupe de G/H et ainsi φ est une application bien définie.

Montrons alors que φ est bijective : supposons que $\varphi(K_1) = \varphi(K_2)$, alors $\forall k \in K_1$, $kH \in K_1/H = K_2/H$, i.e., $\exists k' \in K_2 : kH = k'H$ ainsi $k'^{-1}k \in H \subset K_2$ et alors $k \in K_2$. De même, on montre que $K_2 \subset K_1$ et ainsi $K_1 = K_2$; ceci prouve que φ est injective.

φ est aussi surjective. En effet, Soit T un sous-groupe de G/H, alors $K = s^{-1}(T)$ est un sous-groupe de G (car s est un homomorphisme de groupes). On a $H \subset K$ (car $H = s^{-1}\{\bar{e}\} \subset s^{-1}(T) = K$) et $K/H = s(K) = T$ (car s est surjectif), i.e., $\varphi(K) = T$ et ainsi φ est surjective.

Si K est un sous-groupe distingué de G contenant H, alors, d'après le troisième théorème d'isomorphisme, K/H est un sous-groupe distingué de G/H. Réciproquement, supposons que K/H est

distingué dans G/H et considérons l'homomorphisme $\psi = s' \circ s : G \xrightarrow{s} G/H \xrightarrow{s'} (G/H)/(K/H)$, où s' et s sont les surjections canoniques. Si $x \in \ker\psi$, alors $\psi(x) = (xH)(K/H) = K/H$ d'où $xH \in K/H$ alors $\exists k \in K : xH = kH$, i.e : $k^{-1}x \in H$ d'où $x \in K$ (car $H \subset K$) et par suite $\ker\psi \subset K$. Vu que $K \subset \ker\psi$ alors $K = \ker\psi$ est un sous-groupe distingué de G.

Il est clair que si $K_1 \subset K_2$, alors $K_1/H \subset K_2/H$. Réciproquement, soit $k_1H \in K_1/H$ avec $k_1 \in K_1$ alors $k_1H \in K_2/H$ (car $K_1/H \subset K_2/H$) d'où $\exists k_2 \in K_2 : k_1H = k_2H$ alors $k_2^{-1}k_1 \in H \subset K_2$ et ainsi $k_1 \in K_2$.

Supposons que K_1 et K_2 sont deux sous-groupes de G contenant H tels que $K_1 \subset K_2$ et montrons que, dans ce cas, $[K_2 : K_1] = [K_2/H : K_1/H]$. Soit $\phi : (K_2/K_1)_g \longrightarrow ((K_2/H)/(K_1/H))_g$ définie par : $kK_1 \longmapsto (kH)(K_1/H)$. ϕ est une application bien définie et ϕ est injective. En effet, $kK_1 = k'K_1$ si, et seulement si, $k^{-1}k' \in K_1$ si, et seulement si, $k^{-1}k'H = (kH)^{-1}(k'H) \in K_1/H$ si, et seulement si, $(kH)K_1/H = (k'H)K_1/H$ si, et seulement si, $\phi(kK_1) = \phi(k'K_1)$. ϕ est aussi surjective car $\forall (kH)K_1/H \in ((K_2/H)/(K_1/H))_g$, $\exists kK_1 \in (K_2/K_1)_g$ $(k \in K_2) : \phi(kK_1) = (kH)K_1/H$ ■

Exemple 2.46 *Les sous-groupes de $\mathbb{Z}/4\mathbb{Z}$ sont les sous-groupes de la forme $n\mathbb{Z}/4\mathbb{Z}$ tels que $4\mathbb{Z} \subset n\mathbb{Z}$, i.e., $n/4$ et ainsi les sous-groupes de $\mathbb{Z}/4\mathbb{Z}$ sont $\mathbb{Z}/4\mathbb{Z}$, $2\mathbb{Z}/4\mathbb{Z}$ et $4\mathbb{Z}/4\mathbb{Z} = \{\bar{0}\}$.*

2.4 Groupe symétrique

2.4.1 Définitions et propriétés

Soit n un entier naturel non nul. Rappelons que l'ensemble S_n des bijections de $\mathbb{N}_n = \{1, ..., n\}$ vers lui-même est un groupe pour la composition des applications (cf. 3) de l'exemple 2.2). Ce groupe est appelé **groupe symétrique de degré n** et ses éléments des **permutations** de $\mathbb{N}_n$.

On représente une permutation $\sigma \in S_n$ comme suit : $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$ et pour tout couple de permutations (σ, φ), on notera $\sigma\varphi$ au lieu de $\sigma \circ \varphi$.

Exemple 2.47 *La permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ de S_4 est la permutation de S_4 définie par $\sigma(1) = 4, \sigma(2) = 1, \sigma(3) = 2$ et $\sigma(4) = 3$.*

On considère les deux permutations $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ et $\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ de S_4, alors

$\sigma\varphi$ est la permutation $\sigma\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 4 & 1 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$.

Proposition 2.48 *Le groupe symétrique S_n est d'ordre $n!$.*

Preuve. Utilisons un raisonnement par récurrence sur n : pour n=1, on a $S_1 = \{id\}$. Supposons que le résultat est vrai pour n. Dans S_{n+1}, on considère la relation $\mathcal{R}$ définie de la façon suivante : $\sigma_1 \mathcal{R} \sigma_2$ si, et seulement si, $\sigma_1(n+1) = \sigma_2(n+1)$. la relation $\mathcal{R}$ est évidemment une relation d'équivalence.

Soit $\bar{\sigma} \in S_{n+1}/\mathcal{R}$. Si $\sigma(n+1) = i \in \mathbb{N}_{n+1} = \{1, \dots, n+1\}$, alors $\bar{\sigma}$ contient autant d'éléments que l'ensemble des bijections définies de $\{1, ..., n\}$ vers $\{1, \dots, i-1, i+1, \dots\}$, i.e., $\bar{\sigma}$ contient autant de permutations que S_n et ainsi, d'après l'hypothèse de récurrence, $card(\bar{\sigma}) = n!$.

D'autre part, soit $f : S_{n+1}/\mathcal{R} \longrightarrow \mathbb{N}_{n+1} = \{1, ..., n+1\}, \bar{\sigma} \longmapsto \sigma(n+1)$. En utilisant la définition de la relation $\mathcal{R}$, on montre que f est une application bijective alors $card(S_{n+1}/\mathcal{R}) = n+1$. Vu que les classes d'équivalence forment une partition de S_{n+1} et que ces classes ont un même cardinal égal à $n!$ alors $card(S_{n+1}) = (n+1).n! = (n+1)!$ ■

Remarque 2.49 *Les groupes symétriques S_1 et S_2 sont abéliens. Cependant, le groupe symétrique S_n, avec $n \geq 3$, ne l'est pas (cf. 3) de l'exemple 2.2).*

Définition 2.50 *Soient $r \leq n$, et $i_1, i_2, \ldots, i_r$ des éléments de $\mathbb{N}_n$ deux à deux distincts. On appelle* ***cycle de longueur r****, ou* ***r-cycle****, et on note $(\mathbf{i}_1 \ldots \mathbf{i}_r)$ la permutation c de $\mathbb{N}_n$ telle que $c(i_1) = i_2, c(i_2) = i_3, \ldots, c(i_{r-1}) = i_r, c(i_r) = i_1$ et $c(k) = k$ pour tout $k \notin \{i_1, i_2, \ldots, i_r\}$.*

Deux cycles $c = (i_1 \ldots i_r)$ et $c' = (j_1 \ldots\ j_s)$ sont dits ***disjoints*** *si les deux ensembles $\{i_1, \ldots, i_r\}$ et $\{j_1, \ldots, j_s\}$ sont disjoints.*

Exemple 2.51 $S_3 = \{e, (12), (13), (23), (123), (132)\}$. $|S_3| = 3! = 6$.

Dans un groupe G quelconque, l'équation $ax = b$ (resp. $xa = b$) possède une solution et une seule : $x = a^{-1}b$ (resp. $x = ba^{-1}$) et si $ax = bx$ (resp. $xa = xb$) alors $a = b$. Ainsi, la table d'un groupe fini G est un ***carré latin****, i.e., chaque élément apparait une fois, et une seule, dans chaque ligne et dans chaque colonne.*

La table suivante est la table de S_3 :

↱ ·	e	(12)	(23)	(13)	(123)	(132)
e	e	(12)	(23)	(13)	(123)	(132)
(12)	(12)	e	(123)	(132)	(23)	(13)
(13)	(13)	(123)	(132)	e	(12)	(23)
(23)	(23)	(132)	e	(123)	(13)	(12)
(123)	(123)	(13)	(12)	(23)	(132)	e
(132)	(132)	(23)	(13)	(12)	e	(123)

Remarque 2.52

1) L'unique cycle de longueur 1 est l'identité Id_n.

2) Si $n \geq 2$, un cycle de longueur 2 : $c = (ij)$, s'appelle une ***transposition*** *et se note τ_{ij} : $\tau_{ij}(i) = j, \tau_{ij}(j) = i$ et $\tau_{ij}(k) = k$ pour tout $k \notin \{i, j\}$. On a $\tau_{ij}^2 = Id_n$.*

3) Soit c un cycle. c est de longueur r si, et seulement si, $o(c) = r$.

Proposition 2.53 *Deux cycles disjoints commutent.*

Preuve. Supposons que $c = (i_1 \ldots i_r)$ et $c' = (j_1 \ldots\ j_s)$ sont deux cycles disjoints et soit $k \in \mathbb{N}_n$.

* Si $k \in \{i_1, \ldots, i_r\}$, alors $c'(k) = k$ (car $k \notin \{j_1, \ldots, j_s\}$) et alors $cc'(k) = c(k)$. D'autre part, $c(k) \in \{i_1, \ldots, i_r\}$ car $k \in \{i_1, \ldots, i_r\}$ et $c = (i_1 \ldots i_r)$, d'où $c(k) \notin \{j_1, \ldots, j_s\}$ et alors $c'c(k) = c(k)$.

* De même si $k \in \{j_1, \ldots, j_s\}$

* Si $k \notin \{i_1, \ldots, i_r\} \cup \{j_1, \ldots, j_s\}$, alors $cc'(k) = c'c(k) = k$

Ainsi $cc' = c'c$ ■

Proposition 2.54 *Toute permutation σ de S_n, différente de Id_n, se décompose en produit de cycles disjoints de longueur ≥ 2.*

Preuve. Soit i_1 le plus petit entier qui n'est pas laissé invariant par σ (i_1 existe puisque $\sigma \neq Id_n$). Soit alors r_1 le plus petit entier ≥ 1 tel que $\sigma^{r_1}(i_1) = i_1$ (un tel entier existe puisque $o(\sigma)$ est fini). Posons $c_1 = (i_1\sigma(i_1)\sigma^2(i_1) \ldots \sigma^{r_1-1}(i_1))$ et $X_1 = \mathbb{N}_n - \{i_1, \sigma(i_1), \ldots, \sigma^{r_1-1}(i_1))\}$. (Les entiers $i_1, \sigma(i_1), \sigma^2(i_1), \ldots, \sigma^{r_1-1}(i_1)$ sont deux à deux distincts car $\sigma(i_1) \neq i_1$ et r_1 est le plus petit entier ≥ 1 tel que $\sigma^{r_1}(i_1) = i_1$).

Si $\forall k \in X_1 : \sigma(k) = k$ alors $\sigma = c_1$; sinon soient i_2 le plus petit entier appartenant à X_1 qui n'est pas laissé invariant par σ, r_2 le plus petit entier tel que $\sigma^{r_2}(i_2) = i_2$ et c_2 le r_2-cycle $(i_2\sigma(i_2)\sigma^2(i_2) \ldots \sigma^{r_2-1}(i_2))$. Il est clair que $c_1$et c_2 sont disjoints.

Ce procédé de détermination des cycles c_i est fini et s'arrête au bout de s étapes. On vérifie aisément qu'on a bien $c = c_1c_2 \ldots\ c_s$ avec c_i disjoint de c_j pour $i \neq j$ ■

Corollaire 2.55 *Toute permutation se décompose en produit de transpositions.*

Preuve. En effet, d'après la proposition précédente, il suffit de montrer qu'une telle décomposition existe pour un cycle. Si $c = (i_1 \dots i_r)$, on vérifie aisément qu'on a : $c = \tau_{i_1 i_2} \tau_{i_2 i_3} \dots \tau_{i_{r-1} i_r}$ ■

2.4.2 Signature d'une permutation

Définition 2.56 *Soient $n \geq 2$ et σ une permutation élément de S_n, i et j deux entiers tels que $1 \leq i < j \leq n$. On dit que i et j présentent une **inversion par rapport à** σ (ou simplement une σ-**inversion**) si $\sigma(i) > \sigma(j)$.*

Soit σ une permutation élément de S_n et considérons le produit $\pi = \prod_{1 \leq i < j \leq n} (j - i)$. On pose $\sigma(\pi) = \prod_{1 \leq i < j \leq n} (\sigma(j) - \sigma(i))$. Puisque σ est une bijection, tous les facteurs de π se retrouvent dans $\sigma(\pi)$ une et une seule fois, mais multiplié par un signe moins pour tous les couples (i, j) tels que i et j présentent une σ-inversion.

Définition et Proposition 2.57 *Soient $n \geq 2$ et σ une permutation élément de S_n. On appelle **signature** de σ et on note $\boldsymbol{\epsilon(\sigma)} = \frac{\sigma(\pi)}{\pi} = \pm 1$.*

Exemple 2.58

1) Id_n n'a aucune inversion.

2) 1 et 2 présentent la seule τ-inversion de la transposition $\tau = (12)$.

3) $\epsilon(Id_n) = 1$

4) Supposons que $i < j$ alors $\epsilon(\tau_{ij}) = -1$ car i et j présentent une τ_{ij}-inversion, i et k présentent une τ_{ij}-inversion $\forall k \in \{i+1, ..., j-1\}$ et aussi j et k présentent une τ_{ij}-inversion $\forall k \in \{i+1, ..., j-1\}$.

5) $\epsilon((123)) = \frac{(2-1)(3-1)(3-2)}{(3-2)(1-2)(1-3)} = (-1)^2 = 1$.

Théorème et Définition 2.59 *L'application $\epsilon : S_n \longrightarrow \{-1, 1\}$, $\sigma \longmapsto \epsilon(\sigma)$, où $n \geq 2$, est un homomorphisme de groupes surjectif. Son noyau, noté A_n, est appelé **sous-groupe alterné** de S_n.*

Preuve. Soient σ et φ deux éléments de S_n et déterminons la signautre $\epsilon(\sigma\varphi)$ de la permutation $\sigma\varphi$. On a : $\epsilon(\sigma) = \frac{\sigma(\pi)}{\pi} = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i} = \prod_{1 \leq i < j \leq n} \frac{\sigma(\varphi(j)) - \sigma(\varphi(i))}{\varphi(j) - \varphi(i)}$, alors $\epsilon(\sigma\varphi) = \frac{\sigma\varphi(\pi)}{\pi} = \prod_{1 \leq i < j \leq n} \frac{\sigma(\varphi(j)) - \sigma(\varphi(i))}{j - i} = \prod_{1 \leq i < j \leq n} \frac{\sigma(\varphi(j)) - \sigma(\varphi(i))}{\varphi(j) - \varphi(i)} \times \frac{\varphi(j) - \varphi(i)}{j - i} = \epsilon(\sigma).\epsilon(\varphi)$.

ϵ est surjectif car $1 = \epsilon(Id_n)$ et $-1 = \epsilon(\tau_{ij})$ ■

Corollaire 2.60

(i) Si $n \geq 2$ et σ est un élément de S_n, alors $\epsilon(\sigma) = (-1)^r$, où r est le nombre de transpositions figurant dans une décomposition de σ en produit de transpositions.

(ii) Si $n \geq 2$ alors $|A_n| = \frac{n!}{2}$.

Preuve. (i) Ce résultat est une conséquence immédiate du théorème précédent et du corollaire 2.55.

(ii) D'après le premier théorème d'isomorphisme, on a : $S_n / A_n \simeq \{-1, 1\}$ et ainsi $|A_n| = \frac{n!}{2}$ ■

Remarque 2.61

1) la décomposition d'une permutation en produit de transpositions n'est pas unique ; on a par exemple : $(123) = \tau_{12}\tau_{23} = \tau_{13}\tau_{12} = \tau_{23}\tau_{12}\tau_{23}\tau_{12}$. Par contre et d'après le corollaire 2.60, la parité du nombre des transpositions est la même dans toute décomposition. Ainsi, une permutation σ élément

de A_n, i.e., une permutation σ qui se décompose en produit d'un nombre pair de transpositions, est dite une ***permutation paire*** *alors qu'une permutation n'appartenant pas à A_n, i.e., qui se décompose en produit d'un nombre impair de transpositions est dite* ***permutation impaire****.*

2) A_n est un sous-groupe distingué de S_n (car $A_n = \ker \epsilon$).

Chapitre 3

Anneaux et Corps

3.1 Définitions et Propriétés élémentaires

3.1.1 Définitions et règles de calcul

Définitions 3.1 *Soit A un ensemble muni de deux lois de composition internes + et . On dit que $(A,+,.)$, ou simplement que A est* ***un anneau*** *si :*

(i) $(A,+)$ est un groupe commutatif

*(ii) La loi **.** est associative, ie. $\forall a,b,c \in A : a.(b.c) = (a.b).c$*

*(iii) La loi **.** est distributive par rapport à +, i.e., $\forall a,b,c \in A : a.(b+c) = a.b + a.c$ et $(b+c).a = b.a + c.a$.*

- Si de plus la loi . est commutative, on dit que l'anneau $(A,+,.)$ (ou simplement A) est ***commutatif.***

*- Si un anneau $(A,+,.)$ possède un élément neutre pour la loi **.**, on dit que l'anneau A est* ***unitaire.*** *Dans ce cas, on note 1_A ou simplement 1 cet élément et on l'appelle* ***unité de A.*** *On rappelle que l'élément neutre pour l'addition est noté 0_A ou simplement 0.*

Proposition 3.2 *Si a,b et c sont des éléments arbitraires d'un anneau A alors :*

(i) $a.0 = 0.a = 0$ (On dit que 0 est un élément ***absorbant****)*

(ii) $(-a).b = a.(-b) = -(ab)$

(iii) $(-a).(-b) = ab$

(iv) $a.(b-c) = a.b - a.c$ et $(a-b).c = a.c - b.c$

*(v) Si $ab = ba$, alors $(a+b)^n = \sum_{i=0}^{n} C_n^i a^i b^{n-i}$, où n est un entier naturel non nul (**Formule du binôme de Newton**)*

(vi) Si A est unitaire, alors l'unité 1 est unique et $1 \neq 0$ sauf si $A = \{0\}$, auquel cas l'anneau est dit ***trivial ou nul.***

Preuve. La vérification de ces propriétés est laissée au lecteur (On utilisera par exemple pour (i) le fait que $0 = 0 + 0$...) ∎

Exemple 3.3

1) $(\mathbb{Z},+,.)$ est un anneau commutatif unitaire.

2) $(\mathbb{Z}/n\mathbb{Z},+,.)$ est un anneau commutatif unitaire d'élément unité $\overline{1}$.

3) Si $n \geq 2$, l'ensemble $\mathcal{M}_n(\mathbb{R})$ des matrices carrées d'ordre n à coefficients dans le corps des réels $\mathbb{R}$, muni de l'addition et du produit des matrices, est un anneau unitaire d'élément unité la matrice identité I_n. Cet anneau est un anneau non commutatif. En effet, en notant E_{ij} la matrice de $\mathcal{M}_n(\mathbb{R})$ ayant 1 dans la position (i,j) et 0 ailleurs, on a $E_{11}E_{12} = \delta_{11}E_{12} = E_{12}$ et $E_{12}E_{11} = \delta_{21}E_{11} = 0$.

4) L'ensemble $\mathbb{R}[X]$ des polynômes à une seule indéterminée X à coefficients dans $\mathbb{R}$, muni de l'addition et de la multiplication des polynômes, est un anneau commutatif unitaire d'élément unité le polynôme constant égal à 1.

5) L'ensemble $\mathbb{Z}[i] = \{a+ib \ / \ a,b \in \mathbb{Z}\}$ muni de l'addition et de la multiplication habituelles, est un anneau commutatif unitaire appelé ***anneau des entiers de Gauss****.*

6) Dans $\mathbb{Z}/6\mathbb{Z}$, $B = \{\overline{0}, \overline{2}, \overline{4}\}$ est un anneau commutatif unitaire d'élément unité $\overline{4}$.

7) Soient E un ensemble et $\mathcal{A}(E,A)$ l'ensemble des applications de E dans A muni des deux opérations suivantes : $\forall f,g \in \mathcal{A}(E,A)$: $f+g$ est l'application de E dans A définie par $(f+g)(\alpha) = f(\alpha)+g(\alpha)$; $f.g$ est l'application de E vers A définie par $(f.g)(\alpha) = f(\alpha).g(\alpha)$. $\mathcal{A}(E,A)$ muni de ces deux opérations est un anneau. Si A est unitaire (resp. commutatif) alors l'anneau $\mathcal{A}(E,A)$ est unitaire (resp. commutatif) d'élément unité l'application constante $\alpha \longmapsto 1_A$, $\forall \alpha \in E$.

8) Si A et B sont deux anneaux, alors les opérations suivantes : $\forall (a,b),(a',b') \in A\times B$: $(a,b)+(a',b') = (a+a', b+b')$ et $(a,b).(a',b') = (aa', bb')$ définissent sur $A\times B$ une structure d'anneau appelée ***anneau produit****. Si A et B sont unitaires (resp. commutatifs) alors $A\times B$ est unitaire (resp. commutatif) d'élément unité $(1_A, 1_B)$.*

Dans toute la suite, tous les anneaux considérés sont supposés être <u>unitaires</u> et <u>*non triviaux*</u>.

3.1.2 Eléments particuliers

Soit $(A,+,.)$ un anneau (unitaire et non trivial).

- On dit qu'un élément a de A est **inversible à gauche** (resp. **inversible à droite**) dans A s'il existe un élément b de A (resp. un élément c de A) tel que $ba = 1$ (resp. $ac = 1$).
- Si $ba = 1$ et $ac = 1$, i.e., si a est inversible à gauche et à droite, alors $b = c$. En effet, $b = b(ac) = (ba)c = c$; dans ce cas, on dit que a est **inversible dans** A et on note a^{-1} l'inverse de a.
- Si a et b sont deux éléments <u>non nuls</u> de A tels que $ab = 0$, alors on dit que a (resp. b) est un **diviseur de zéro à droite** (resp. **diviseur de zéro à gauche**).
- Un élément a de A est dit un **diviseur de zéro** si a est à la fois diviseur de zéro à droite et à gauche.

Remarque 3.4

1) L'ensemble $\mathcal{U}(A)$ des éléments inversibles de A, muni de la multiplication, est un groupe appelé ***groupe des éléments inversibles de*** *A ou* ***groupe des unités de*** *A.*

2) Dans un anneau <u>commutatif</u>, les notions d'éléments inversibles à droite et à gauche coincident. Dans ce cas, on parle alors simplement d'éléments inversibles.

3) Dans un anneau <u>commutatif</u>, les notions de diviseurs de zéro à droite et à gauche coincident. Dans ce cas, on parle alors simplement de diviseurs de zéro.

Exemple 3.5

1) $\mathcal{U}(\mathbb{Z}) = \{-1,1\}$, $\mathcal{U}(\mathbb{Z}/n\mathbb{Z}) = \{\overline{x} \in \mathbb{Z}/n\mathbb{Z} \ / \ x \wedge n = 1\}$.

2) $\mathcal{U}(\mathcal{M}_n(\mathbb{R})) = Gl_n(\mathbb{R}) = \{M \in \mathcal{M}_n(\mathbb{R}) / \det M \neq 0\}$.

3) Dans $\mathcal{M}_n(\mathbb{R})$, on a : $E_{12}E_{11} = 0$ et $E_{11}E_{21} = 0$ d'où E_{11} est un diviseur de zéro à gauche et à droite dans $\mathcal{M}_n(\mathbb{R})$.

3.1.3 Anneau intègre

Définition 3.6 *Un anneau <u>commutatif</u> $(A,+,.)$ est dit* ***anneau intègre*** *si A ne possède pas de diviseurs de zéro, i.e., si $ab = 0$ alors $a = 0$ ou $b = 0$.*

Exemple 3.7

1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ *et* $\mathbb{C}$ *sont des anneaux intègres.*

2) $\mathbb{Z}/p\mathbb{Z}$*, où* p *est un nombre premier, est un anneau intègre.*

3) $\mathbb{Z}/4\mathbb{Z}$ *n'est pas un anneau intègre (on a* $\overline{2}.\overline{2}=\overline{0}$*).*

3.1.4 Sous-anneau

Définition 3.8 *Soit* $(A, +, .)$ *un anneau et* B *une partie de* A*. On dit que* B *est un* ***sous-anneau*** *de l'anneau* $(A, +, .)$ *si :*

(i) $1_A \in B$

(ii) B *est stable pour les les deux lois de composition internes* $+, .$ *et* $(B, +, .)$ *est un anneau.*

Proposition 3.9 *Soit* A *un anneau et* B *une partie de* A*.* B *est un sous-anneau de* A *(au sens des anneaux unitaires) si, et seulement si :*

(i) $1_A \in B$

(ii) $\forall a, b \in B,\ a - b \in B$

(iii) $\forall a, b \in B,\ ab \in B$

Exemple 3.10

1) $\mathbb{Z}$ *est un sous-anneau de* $\mathbb{Q}$*.*

2) Le seul sous-anneau de $\mathbb{Z}$ *est* $\mathbb{Z}$ *lui-même. En effet, si* B *est un sous-anneau de* $\mathbb{Z}$*, alors* $1 \in B$*,* $2 = 1 + 1 \in B, ...$*et* $\forall n \in \mathbb{N}^*, n = 1 + ... + 1 \in B$*.* $0 = 1 - 1 \in B$*, aussi* $\forall n \in \mathbb{N}^*, -n = 0 - n \in B$ *et ainsi* $B = \mathbb{Z}$*.*

3) Dans $\mathbb{R}[X]$*, l'ensemble* $\mathbb{R}[X^2] = \{P(X^2)/P(X) \in \mathbb{R}[X]\}$ *est un sous-anneau de* $\mathbb{R}[X]$*.*

4) Dans $\mathcal{M}_n(\mathbb{R})$*, l'ensemble* $D_n(\mathbb{R})$ *des matrices diagonales et l'ensemble* $T_n(\mathbb{R})$ *des matrices triangulaires supérieur sont des sous-anneaux de* $\mathcal{M}_n(\mathbb{R})$*.*

5) Si A *est un anneau, alors* $\{0_A\}$ *n'est pas un sous-anneau de* A*. Tandis que* $\{x \in A/\ \exists n \in \mathbb{Z} : x = n.1_A\}$ *est un sous-anneau de* A*.*

Remarque 3.11

1) En général, un anneau B *contenu dans un anneau* A *n'est pas nécessairement un sous-anneau de* A *(au sens des anneaux unitaires). L'anneau* $B = \{\overline{0}, \overline{2}, \overline{4}\}$ *n'est pas un sous-anneau de l'anneau* $A = \mathbb{Z}/6\mathbb{Z}$ *(au sens des anneaux unitaires) car* $1_A = \overline{1} \notin B$*.*

2) Un sous-anneau d'un anneau intègre est intègre.

3.1.5 Caractéristique d'un anneau

Soit (A,+,.) un anneau. Pour $n \in \mathbb{Z}$ et $a \in A$, on définit
$$na = \begin{cases} \overbrace{a + \cdots + a}^{n \text{ fois}} & \text{si } n > 0 \\ 0 & \text{si } n = 0 \\ \overbrace{(-a) + \cdots + (-a)}^{-n \text{ fois}} & \text{si } n < 0 \end{cases}$$

Si $n, m \in \mathbb{Z}$ et $a \in A$ alors $(n + m).a = na + ma$ et $(nm)a = n(ma)$.

On définit **la caractéristique d'un anneau** A comme étant le plus petit entier $n > 0$ tel que $n.1_A = 0_A$ si un tel entier existe. Sinon (i.e., si $\forall n \in \mathbb{N}^* : n.1_A \neq 0_A$), on dit que la caractéristique de l'anneau A est nulle. La caractéristique de l'anneau A est notée $car(A)$.

Exemple 3.12

1) $car(\mathbb{Z}) = 0$*.*

2) Si $n \geq 2$*,* $car(\mathbb{Z}/n\mathbb{Z}) = n$*.*

Remarque 3.13 *Soit $(A,+,.)$ un anneau.*

1) Dans le groupe commutatif $(A,+)$, si 1_A est d'ordre fini, alors $car(A) = \circ(1)$. Sinon, $car(A) = 0$.

2) $car(A) \neq 1$ (car A est non trivial).

3) Si B est un sous-anneau de A, alors $car(B) = car(A)$.

4) Si A est intègre et $car(A) \neq 0$, alors $car(A)$ est un nombre premier. En effet, posons $car(A) = n = st$, où s et t sont deux entiers naturels alors $s \leq n$ et $t \leq n$. On a : $n.1_A = (st).1_A = (s.1_A)(t.1_A) = 0_A$, alors $s.1_A = 0_A$ ou $t.1_A = 0_A$ (car A est intègre) et ainsi $s = n$ ou $t = n$ (car n est le plus petit entier naturel non nul tel que $n.1_A = 0_A$).

5) $car(A)$ est le plus petit entier $n > 0$ tel que $n.a = 0_A$, $\forall a \in A$, si un tel entier existe ; sinon, $car(A) = 0$.

3.2 Corps

Définition 3.14 *Soit $(K,+,.)$ un anneau <u>commutatif</u> (unitaire et non trivial). On dit que $(K,+,.)$ est un **corps** (commutatif) si tout élément non nul de K est inversible.*

Exemple 3.15

1) $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps.

2) $\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, n est un nombre premier.

3) $\mathbb{Z}$ est un anneau intègre qui n'est pas un corps.

Propriétés 3.16

*(i) Si K est un corps, alors K est intègre et $\mathcal{U}(K) = K^* = K - \{0\}$ est un groupe pour la multiplication appelé **groupe multiplicatif** du corps K.*

(ii) Si K est un corps, alors $car(K) = 0$ ou $car(K) = p$, où p est un nombre premier.

Définition 3.17 *Soit $(K,+,.)$ un corps et L un <u>sous-anneau</u> de $(K,+,.)$. On dit que L est un **sous-corps** du corps $(K,+,.)$ si $(L,+,.)$ est un corps.*

*On dit que L est un **sous-corps propre** de K si L est un sous-corps de K différent de K.*

Proposition 3.18 *Soit $(K,+,.)$ un corps et L une partie de K. L est un sous-corps du corps $(K,+,.)$ si, et seulement si :*

(i) L est un sous-anneau de K

(ii) Pour tout $a \in L - \{0\}$, $a^{-1} \in L$.

Exemple 3.19

1) $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$ et $\mathbb{R}$ est un sous-corps de $\mathbb{C}$.

2) $\mathbb{Q}$ ne possède pas de sous-corps propre. En effet, soit L un sous-corps de $\mathbb{Q}$, alors $0, 1 \in L$ d'où $\forall n \in \mathbb{Z}, n \in L$. comme L est un corps alors $\forall n \in \mathbb{Z}^*, n^{-1} \in L$. Soit $x \in \mathbb{Q}$, alors x s'écrit sous la forme $\frac{m}{n}$ avec $(m,n) \in \mathbb{Z} \times \mathbb{Z}^*$ donc $x = \frac{m}{n} = mn^{-1} \in L$ et $L = \mathbb{Q}$.

Exercice 3.20 *Soit $d \in \mathbb{N}$.*

1) Montrer que $\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} \;/ a, b \in \mathbb{Q}\}$ est un sous-corps de $\mathbb{R}$.

2) Quels sont les sous-corps de $\mathbb{Q}[\sqrt{d}]$?

3.3 Idéaux, Homomorphismes et Anneaux quotients

3.3.1 Idéaux et homomorphismes

Définition 3.21 *Soit $(A,+,.)$ et $(B,+,.)$ deux anneaux (unitaires et non triviaux). On dit qu'une application f de A dans B est un* ***homomorphisme d'anneaux*** *(ou* ***morphisme d'anneaux****) si :*

(i) $f(x+y)=f(x)+f(y)$ pour tout (x,y) élément de A^2

(ii) $f(x.y)=f(x).f(y)$ pour tout (x,y) élément de A^2

(iii) $f(1_A)=1_B$

*On définit, d'une manière analogue à celle des groupes, les notions d'****endomorphisme****, d'****isomorphisme*** *et d'****automorphisme d'anneaux****. Si f est un isomorphisme,on dit que A et B sont* ***isomorphes*** *et on note* $\mathbf{A}\simeq\mathbf{B}$.

Exemple 3.22

1) L'application canonique $s:\mathbb{Z}\longrightarrow\mathbb{Z}/n\mathbb{Z}$, $m\longmapsto s(m)=\overline{m}$ est un homomorphisme d'anneaux surjectif.

2) Si $n\wedge m=1$, alors $f:\mathbb{Z}/nm\mathbb{Z}\longrightarrow\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$ définie par $f(\hat{a})=(\bar{a},\dot{a})$ est un isomorphisme d'anneaux ($\hat{a}=a+nm\mathbb{Z}$ est la classe de a modulo $nm\mathbb{Z}$, $\bar{a}=a+n\mathbb{Z}$ est la classe de a modulo $n\mathbb{Z}$ et $\dot{a}=a+m\mathbb{Z}$ est la classe de a modulo $m\mathbb{Z}$).

3) Soit f l'application définie de $\mathbb{Z}$ vers $\mathcal{M}_n(\mathbb{R}), n\geq 2$, par $f(m)=mE_{11}$. f vérifie les conditions : $f(n+m)=f(n)+f(m)$ et $f(nm)=f(n)f(m)$, mais f n'est pas un homomorphisme d'anneaux (au sens des anneaux unitaires) car $f(1)\neq I_n$.

Proposition 3.23

(i) Si $f:A\longrightarrow B$ et $g:B\longrightarrow C$ sont deux homomorphismes d'anneaux, alors la composée $g\circ f:A\longrightarrow C$ est un homomorphisme d'anneaux

(ii) Si $f:A\longrightarrow B$ est un isomorphisme, alors f^{-1} est un isomorphisme de B vers A.

(iii) Soit $f:A\longrightarrow B$ un homomorphisme d'anneaux.

** Si A' est un sous-anneau de A, alors $f(A')$ est un sous-anneau de B. En particulier, $\operatorname{Im} f=f(A)$ est un sous-anneau de B.*

** Si B' est un sous-anneau de B, alors $f^{-1}(B')$ est un sous-anneau de A.*

Définitions 3.24

- Soit $(A,+,.)$ un anneau et I une partie de A. On dit que I est un ***idéal à gauche*** *(resp.* ***idéal à droite****) de l'anneau A si :*

(i) I est un sous-groupe du groupe additif $(A,+)$

(ii) Pour tout a élément de A : $aI\subseteq I$, i.e., $\forall a\in A$, $\forall x\in I$, alors $ax\in I$ (resp. pour tout a élément de A, $Ia\subseteq I$, i.e., $\forall a\in A$, $\forall x\in I$, alors $xa\in I$).

- Si I est un idéal à la fois à gauche et à droite de A, alors on dit que I est un ***idéal bilatère*** *(ou simplement un* ***idéal****) de A.*

- A et $\{0_A\}$ sont des idéaux de A appelés ***idéaux triviaux*** *de A.*

- Un idéal I de A différent de A est appelé ***idéal propre*** *de A.*

Proposition 3.25 *Soit $(A,+,.)$ un anneau et I une partie de A. I est un idéal à gauche (resp. idéal à droite) de l'anneau A si, et seulement si :*

(i) $I\neq\emptyset$

(ii) $\forall x,y\in I: x-y\in I$

(iii) $\forall a\in A,\forall x\in I: ax\in I$ (resp. $xa\in I$).

Exemple 3.26

1) Les idéaux de $\mathbb{Z}$ *sont de la forme* $n\mathbb{Z}$.

2) Dans $\mathcal{M}_n(\mathbb{R})$, $n \geq 2$, *l'ensemble* I *des matrices dont la première colonne est nulle est un idéal à gauche de* $M_n(\mathbb{R})$ *(mais* I *n'est pas un idéal à droite de* $\mathcal{M}_n(\mathbb{R})$*) et l'ensemble* J *des matrices dont la première ligne est nulle est un idéal à droite de* $M_n(\mathbb{R})$ *(mais* J *n'est pas un idéal à gauche de* $\mathcal{M}_n(\mathbb{R})$*).*

Propriétés 3.27

(i) Si I *est un idéal à gauche (resp. à droite) de* A, *alors* $I = A$ *si, et seulement si,* $\exists\, u \in \mathcal{U}(A)$: $u \in I$ *si, et seulement si,* $1 \in A$.

(ii) Si l'anneau A *est commutatif, alors les notions d'idéaux à gauche, idéaux à droite et idéaux bilatères coincident.*

(iii) L'intersection $\bigcap_{k \in E} I_k$ *d'une famille quelconque* $(I_k)_{k \in E}$ *d'idéaux est un idéal.*

(iv) Si I *et* J *sont deux idéaux de* A, *alors l'ensemble* $I + J = \{x + y \ / \ x \in I \text{ et } y \in J\}$ *est un idéal de* A *appelé* ***idéal somme*** *de* I *et de* J.

Proposition et Définition 3.28 *Soit* X *une partie d'un anneau* A. *L'idéal de* A *intersection des idéaux de* A *contenant* X *est appelé* ***idéal de*** A ***engendré par*** X *et est noté* $< \mathbf{X} >$. *Cet idéal est aussi le plus petit idéal de* A *contenant* X.

Exemple 3.29

1) $< \varnothing >= \{0\}$ *et* $< \{1\} >= A$.

2) Si A *est commutatif et* $x \in A$, *alors* $< \{x\} >= Ax = \{ax/a \in A\}$ *et est noté* $< x >$ *ou* (x).

3) Soient I *et* J *deux idéaux de* A. *L'idéal de* A *engendré par* $I \cup J$ *est l'idéal* $I + J$.

4) Soient I, J *deux idéaux de* A *et* $X = \{xy/x \in I \text{ et } y \in J\}$. *En général,* X *n'est pas un idéal de* A *et* $< X >$ *est l'idéal* $\{\sum_{i=1}^{n} x_i y_i / n \in \mathbb{N}^* \text{ et } \forall i = 1, ..., n : x_i \in I, y_i \in J\}$ *noté* $I.J$ *et appelé* ***idéal produit*** *des deux idéaux* I *et* J.

Exercice 3.30 *Soient* A *un anneau commutatif (unitaire),* u, a *et* b *des éléments de* A. *Montrer que*

1) $u \in \mathcal{U}(A)$ *si, et seulement si,* $(u) = A$.

2) $(x) \subset (y)$ *si, et seulement si,* $\exists a \in A : x = ay$.

Définitions 3.31

- Un idéal I *d'un anneau* A *est dit* ***idéal principal*** *s'il existe un élément* x *de* A *tel que* $I =< x >= (x)$.

- Si dans un anneau intègre A, *tout idéal est principal, on dit que* A *est un* ***anneau principal***.

Exemple 3.32

1) $\{0\} =< 0 >$ *et* $A =< 1 >$ *sont des idéaux principaux.*

2) $\mathbb{Z}$ *est un anneau principal.*

Exercice 3.33 *Soit* X *une partie d'un anneau commutatif* A. *Montrer que*

1) si I *est un idéal de* A, *alors* $< X > \subset I$ *si, et seulement si,* $X \subset I$.

2) $< X >= \{\sum_{i=1}^{n} a_i x_i / \ n \in \mathbb{N}^*, x_1, ..., x_n \in X, a_1, ..., a_n \in A\}$.

3) Si $X = \{x_1, ..., x_n\}$ *est finie, alors* $< X >= Ax_1 + ... + Ax_n = (x_1) + ... + (x_n)$.

Proposition 3.34 *Soient* A, B *deux anneaux et* $f : A \longrightarrow B$ *un homomorphisme d'anneaux.*

(i) Si J *est un idéal de* B, *alors* $f^{-1}(J)$ *est un idéal de* A. *En particulier,* $f^{-1}(\{0\}) = \ker f$ *est un idéal de* A *appelé* ***noyau de l'homomorphisme*** f.

(ii) f *est injectif si, et seulement si,* $\ker f = \{0\}$.

3.3.2 Anneaux quotients

Soit A un anneau et I un idéal de A. Puisque $(A,+)$ est un groupe abélien et I est un sous-groupe de $(A,+)$, l'ensemble A/I des classes d'équivalence modulo I définies par la relation : $a\mathcal{R}b \Longleftrightarrow a-b \in I$, muni de l'addition, est un groupe abélien (cf. chapitre II).

Dans ce groupe, on définit la multiplication de la façon suivante : $\forall \overline{a} = a+I, \overline{b} = b+I \in A/I$: $\overline{a}.\overline{b} = \overline{ab} = ab+I$. Cette opération est bien définie ; en effet, soient $a', b' \in A$ tels que $\overline{a'} = \overline{a}$ et $\overline{b'} = \overline{b}$ alors $a'b' - ab = a'b' - ab' + ab' - ab = (a'-a)b' + a(b'-b) \in I$, car $(a'-a), (b'-b) \in I$ et I est un idéal de A, d'où $\overline{a'b'} = \overline{ab}$ et ainsi, la multiplication des classes d'équivalence est indépendante des représentants choisis.

En utilisant les propriétés d'anneau de A, on vérifie facilement que $(A/I,+,.)$ est un anneau, $\overline{0}$ est l'élément zéro de A/I et $\overline{1}$ est l'unité de A/I.

l'anneau A/I est trivial si, et seulement si, $I = A$.

Définition 3.35 *Soit A un anneau et I un idéal de A. L'anneau $(A/I,+,.)$ est appelé* ***l'anneau quotient de l'anneau A par l'idéal I****.*

3.4 Théorèmes d'isomorphismes

Théorème 3.36 (Premier théorème d'isomorphisme) *Si $f : A \longrightarrow B$ est un homomorphisme d'anneaux, alors les anneaux $A/\ker f$ et $\operatorname{Im} f$ sont isomorphes.*

Preuve. Soit $\overline{f} : A/\ker f \longrightarrow \operatorname{Im} f$ définie par $\overline{f}(\overline{x}) = f(x)$. On sait que $\overline{f}$ est un isomorphisme de groupes (cf. le premier théorème d'isomorphisme pour les groupes). D'autre part, on a $\overline{f}(\overline{1_A}) = f(1_A) = 1_B$ et $\forall \overline{x}, \overline{y} \in A/\ker f$: $\overline{f}(\overline{x}\ \overline{y}) = \overline{f}(\overline{xy}) = f(xy) = f(x)f(y) = \overline{f}(\overline{x})\overline{f}(\overline{y})$ et ainsi f est un isomorphisme d'anneaux ■

Théorème 3.37 (Deuxième théorème d'isomorphisme) *Soit A un anneau, I un idéal de A et B un sous-anneau de A, alors :*

(i) $B+I = \{b+x \ / \ b \in B$ et $x \in I\}$ est un sous-anneau de A et I est un idéal de $B+I$.

(ii) $B \cap I$ est un idéal de B.

(iii) Les anneaux $(B+I)/I$ et $B/B \cap I$ sont isomorphes.

Preuve.

(i) $1_A = 1_A + 0 \in B+I$. $\forall b_1 + x_1, b_2 + x_2 \in B+I$ $(b_i \in B, x_i \in I)$, alors $(b_1+x_1) - (b_2+x_2) = (b_1-b_2) + (x_1-x_2) \in B+I$ et $(b_1+x_1)(b_2+x_2) = b_1b_2 + (b_1x_2 + x_1b_2 + x_1x_2) \in B+I$ donc $B+I$ est un sous-anneau de A. On vérifie facilement que I est un idéal de $B+I$.

(ii) et (iii). Soit s la surjection canonique $s : A \longrightarrow A/I$, $s(x) = \overline{x}$. On considère la restriction de s à B, $s' : B \longrightarrow A/I$, $x \longmapsto s'(x) = s(x)$. s' est évidemment un homomorphisme d'anneaux. On a $\ker s' = B \cap I$ et ainsi $B \cap I$ est un idéal de B. On a aussi $\operatorname{Im} s' = (B+I)/I$ (cf. chapitre II, le deuxième théorème d'isomorphisme pour les groupes). Ainsi, le premier théorème d'isomorphisme donne : $B/(B \cap I) \simeq (B+I)/I$ ■

Théorème 3.38 (Troisième théorème d'isomorphisme) *Soit A un anneau, I et J deux idéaux de A tels que $I \subseteq J$.*

1) J/I est un idéal de A/I

2) Les anneaux A/J et $(A/I)\diagup(J/I)$ sont isomorphes.

Preuve. Soit $f : A/I \longrightarrow A/J$, $\overline{x} \longmapsto f(\overline{x}) = \widehat{x}$ où $\overline{x}$ (resp. $\widehat{x}$) désigne la calsse de x modulo I (resp. modulo J). On sait que f est un homomorphisme de groupes surjectif et que $\ker f = J/I$ (cf. le

troisième théorème d'isomorphisme pour les groupes). D'autre part, on a : $f(\overline{1}) = \widehat{1}$ et $\forall \overline{x}, \overline{y} \in A/I$: $f(\overline{x}\,\overline{y}) = \widehat{xy} = \widehat{x}\widehat{y} = f(\overline{x})f(\overline{y})$, ainsi f un homomorphisme d'anneaux surjectif, alors $\ker f = J/I$ est un idéal de A/I et d'après le premier théorème d'isomorphisme, $A/I \diagup J/I \simeq A/J$ ■

Théorème 3.39 (Théorème de correspondance pour les anneaux) *Soit I un idéal d'un anneau A.*

(i) L'application $B \longmapsto B/I$ définie une correspondance biunivoque entre l'ensemble des sous-anneaux de A contenant I et les sous-anneaux de A/I, i.e., C est un sous-anneau de A/I si, et seulement si, il existe un sous-anneau B de A contenant I tel que $C = B/I$.

(ii) L'application $J \longmapsto J/I$ définie une correspondance biunivoque entre l'ensemble des idéaux de A contenant I et l'ensemble des idéaux de A/I, i.e., K est un idéal de A/I si, et seulement si, il existe un idéal J de A contenant I tel que $K = J/I$.

Preuve. Montrons par exemple (ii). Soit $\varphi : \{J/\ J$ est un idéal de A contenant $I\} \longrightarrow \{K/\ K$ est un idéal de $A/I\}$ définie par : $\varphi(J) = J/I$.

Si J est un idéal de A contenant I, alors J est un sous-groupe du groupe $(A, +)$ contenant le sous-groupe I de $(A, +)$ et ainsi, d'après le théorème de correspondance pour les groupes, $\varphi(J) = J/I$ est un sous-groupe du groupe quotient $(A/I, +)$. En vérifiant que $\forall \bar{a} \in A/I, \forall \bar{x} \in J/I$, $\bar{a}\bar{x} = \overline{ax} \in J/I$, on a J/I est un idéal de l'anneau quotient A/I et ainsi φ est une application bien définie.

Montrons alors que φ est bijective : φ est injective (cf le théorème de correspondance pour les groupes).

φ est aussi surjective. En effet, Soit K un idéal de A/I, alors $J = s^{-1}(K)$ est un idéal de A (car $s : A \longrightarrow A/I, x \longmapsto \bar{x}$ est un homomorphisme d'anneaux) et on a $I \subset J$ (car $I = s^{-1}\{\bar{0}\} \subset s^{-1}(K) = J$) et $J/I = s(J) = K$ (car s est surjectif), i.e., $\varphi(J) = K$ et ainsi φ est surjective ■

Exercice 3.40 *Montrer que $\mathbb{Z}/p\mathbb{Z}$, où p est un nombre premier, ne possède pas de sous-corps propre.*

Exercice 3.41 *Soit K un corps (commutatif).*

1)

a) Montrer que l'intersection des sous-corps de K est un sous- corps de K. On l'appelle le sous-corps premier de K et on le note $P(K)$.

b) Montrer que $P(K) = \{(n.1_K).(m.1_K)^{-1}/\ n, m \in \mathbb{Z}$ et $m.1_K \neq 0_K\}$.

2) On considère l'application $f : \mathbb{Z} \longrightarrow K$, $n \longmapsto n.1_K$.

a) Vérifier que f est un homomorphisme d'anneaux.

b) Montrer que si $carK = p$, où p est un nombre premier, alors $P(K) \simeq \mathbb{Z}/p\mathbb{Z}$.

c) Montrer que si $carK = 0$, alors $P(K) \simeq \mathbb{Q}$.

3.5 Idéaux Premiers et idéaux maximaux

Dans toute la suite, nous supposons que A est un anneau commutatif (unitaire et non trivial).

Définition 3.42 *Soit $\mathfrak{p}$ un idéal de A. On dit que $\mathfrak{p}$ est un* ***idéal premier*** *de A si :*

(i) $\mathfrak{p} \neq A$

(ii) $\forall a, b \in A$: si $ab \in \mathfrak{p}$, alors $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$.

Théorème 3.43 *Soit $\mathfrak{p}$ un idéal de A. $\mathfrak{p}$ est un idéal premier de A si, et seulement si, $A/\mathfrak{p}$ est un anneau intègre.*

Preuve. Supposons que $\mathfrak{p}$ est premier, alors $A/\mathfrak{p}$ est un anneau commutatif (non trivial, car $\mathfrak{p} \neq A$, et unitaire). Si $\overline{a}\overline{b} = \overline{0}$, alors $ab \in \mathfrak{p}$ d'où $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$, i.e., $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$. Réciproquement, si $A/\mathfrak{p}$ est un anneau intègre, alors $\mathfrak{p} \neq A$ et si $ab \in \mathfrak{p}$, ie. $\overline{a}\overline{b} = \overline{ab} = \overline{0}$, alors, puisque $A/\mathfrak{p}$ est intègre, $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$, i.e., $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$ ■

Définition 3.44 *Soit $\mathfrak{m}$ un idéal de A. On dit que $\mathfrak{m}$ est un* ***idéal maximal*** *de A si :*
(i) $\mathfrak{m} \neq A$
(ii) Il n'existe aucun idéal propre de A contenant $\mathfrak{m}$ autre que $\mathfrak{m}$, i.e., si I est un idéal de A tel que $\mathfrak{m} \subset I$, alors $I = \mathfrak{m}$ ou $I = A$.

Théorème 3.45 *Soit $\mathfrak{m}$ un idéal de A. Alors $\mathfrak{m}$ est un idéal maximal de A si, et seulement si, $A/\mathfrak{m}$ est un corps.*

Preuve. Supposons que $\mathfrak{m}$ est maximal. Alors $A/\mathfrak{m}$ est un anneau commutatif (non trivial, car $\mathfrak{m} \neq A$) et unitaire. Si $\overline{a} \in A/\mathfrak{m}$ est tel que $\overline{a} \neq \overline{0}$, i.e., $a \notin \mathfrak{m}$, alors l'idéal $< a > +\mathfrak{m} \neq \mathfrak{m}$. Ainsi $< a > +\mathfrak{m} = A$ car $\mathfrak{m}$ est maximal et $\mathfrak{m} \subsetneq < a > +\mathfrak{m}$. D'où $\exists\ r \in A, \exists\ x \in \mathfrak{m} : 1 = ra + x$, alors $\overline{1} = \overline{ra} = \overline{ra}$ dans $A/\mathfrak{m}$ ($\bar{x} = \bar{0}$ car $x \in m$). Ceci prouve que $\overline{a}$ est inversible dans $A/\mathfrak{m}$ et que $A/\mathfrak{m}$ est un corps. Réciproquement, si $A/\mathfrak{m}$ est un corps, alors $\mathfrak{m} \neq A$. Soit I un idéal de A tel que $\mathfrak{m} \subsetneq I$ et soit $x \in I - \mathfrak{m}$. Alors $\overline{x} \neq \overline{0}$ dans $A/\mathfrak{m}$ d'où $\exists\ y \in A$ tel que $\overline{x}\ \overline{y} = \overline{xy} = \overline{1}$, ainsi $1 - xy \in \mathfrak{m} \subset I$ et par suite $1 \in I$ (car $x \in I$), i.e., $I = A$ ■

Corollaire 3.46 *Tout idéal maximal est premier*

Exemple 3.47
1) Dans l'anneau $\mathbb{Z}$, si p est un nombre premier, alors $p\mathbb{Z}$ est un idéal maximal (et alors premier).
2) Dans $\mathbb{Z}$, L'idéal (0) est premier, mais non maximal.

Exercice 3.48 *Soit $n \in \mathbb{N}^*$. Montrer que les propositions suivantes sont équivalentes :*
(i) $n\mathbb{Z}$ est un idéal maximal
(ii) $n\mathbb{Z}$ est un idéal premier
(iii) n est un nombre premier

Exercice 3.49 *Soit A un anneau commutatif. Montrer que A est intègre si, et seulement si, (0) est un idéal premier.*

Exercice 3.50 *Soit K un anneau commutatif. Montrer que les propositions suivantes sont équivalentes :*
(i) K est un corps
(ii) (0) est un idéal maximal de K
(iii) Les seuls idéaux de K sont $\{0\}$ et K
(iv) Tout homomorphisme d'anneaux $f : K \longrightarrow B$, où B est un anneau, est injectif.

Exercice 3.51 *Soient A un anneau commutatif et I un idéal de A.*
1) Montrer que si $\mathfrak{p}$ (resp. $\mathfrak{m}$) est un idéal premier (resp. idéal maximal) de A contenant I, alors $\mathfrak{p}/I$ (resp. $\mathfrak{m}/I$) est un idéal premier (resp. maximal) de A/I.
2) Montrer que si $\mathfrak{p}'$ (resp. $\mathfrak{m}'$) est un idéal premier (resp. idéal maximal) de A/I, alors il existe un idéal premier $\mathfrak{p}$ (resp. un idéal maximal $\mathfrak{m}$) de A, contenant I, tel que $\mathfrak{p}' = \mathfrak{p}/I$ (resp. $\mathfrak{m}' = \mathfrak{m}/I$).

3.6 Corps des fractions d'un anneau intègre

Soit A un anneau intègre.

Théorème et Définition 3.52 *Il existe un corps K et un homomorphisme injectif $f : A \to K$ tels que $K = \{f(a)(f(b))^{-1}/a \in A, b \in A - \{0\}\}$.*
De plus, si K' est un corps et $g : A \longrightarrow K'$ un homomorphisme injectif tels que $K' = \{g(a)(g(b))^{-1}/a \in A, b \in A - \{0\}\}$ alors $K \simeq K'$.
Le corps K, unique à un isomorphisme près, est appelé ***le corps des fractions de l'anneau intègre A*** *et est noté* $\mathbf{Fr(A)}$.

Preuve. Dans $B = A \times A^*$, on définit la relation $\mathcal{R}$ suivante : $\forall (a,b),(c,d) \in B : (a,b)\mathcal{R}(c,d)$ si, et seulement si, $ad = bc$. On vérifie facilement que $\mathcal{R}$ est une relation d'équivalence.

Soit $K = B/\mathcal{R} = \{\overline{(a,b)}/(a,b) \in B\}$ l'ensemble quotient associé à la relation $\mathcal{R}$. On vérifie que l'addition et la multiplication définies comme suit sont indépendantes des representants des classes

$$\overline{(a,b)} + \overline{(c,d)} = \overline{(ad+bc, bd)}$$
$$\overline{(a,b)}.\overline{(c,d)} = \overline{(ac, bd)}$$

($bd \in A^*$ car $b \neq 0, d \neq 0$ et A est intègre).

On vérifie aussi que ces deux lois définissent sur l'ensemble K une structure d'anneau commutatif, son élément zéro est $\overline{(0,1)}$ $(= \overline{(0,d)}, \forall d \in A^*)$ et son élément unité est $\overline{(1,1)}$ $(= \overline{(d,d)}, \forall d \in A^*)$. De plus, K est un corps. En effet, soit $\overline{(a,b)} \neq \overline{(0,1)}$, alors $a \in A^*$ d'où $(b,a) \in B$, $\overline{(a,b)}.\overline{(b,a)} = \overline{(ab,ba)} = \overline{(1,1)}$ et $\overline{(a,b)}$ est inversible d'inverse $\overline{(b,a)}$, et par conséquent K est un corps.

Considérons l'application

$$\begin{array}{rccc} f: & A & \longrightarrow & K \\ & a & \longmapsto & \overline{(a,1)} \end{array}$$

f est un homomorphisme d'anneaux injectif. En effet, $f(a+a') = \overline{(a+a',1)} = \overline{(a,1)} + \overline{(a',1)} = f(a) + f(a')$; $f(a.a') = \overline{(aa',1)} = \overline{(a,1)}\ \overline{(a',1)} = f(a)f(a')$ et $f(1) = \overline{(1,1)} = 1_K$. Soit maintenant $a \in \ker f$, alors $f(a) = \overline{(a,1)} = \overline{(0,1)}$, i.e., $a \times 1 = 1 \times 0 = 0$ et ainsi f est un homomorphisme injectif.

Soit K' un corps et $g : A \longrightarrow K'$ un homomorphisme d'anneaux injectif tels que $K' = \{g(a)(g(b))^{-1}/a \in A, b \in A - \{0\}\}$.

On considère $\varphi : K \longrightarrow K'$ définie par $\varphi(\overline{(a,b)}) = g(a)(g(b))^{-1}$. φ est une application bien définie. En effet, si $\overline{(a,b)} = \overline{(c,d)}$, i.e., $ad = bc$, alors $g(ad) = g(cb)$ et $g(a)g(d) = g(c)g(b)$. D'autre part, puisque b et d sont non nuls, alors $g(b)$ et $g(d)$ sont aussi non nuls dans K', car g est injectif, et donc $g(b)$ et $g(d)$ sont inversibles dans le corps K'. Par conséquent, $\varphi(\overline{(a,b)}) = g(a)(g(b))^{-1} = g(c)(g(d))^{-1} = \varphi(\overline{(c,d)})$.

On vérifie facilement que φ est un homomorphisme d'anneaux. φ est par construction, surjectif.

D'autre part, φ est aussi injectif. En effet, si $\overline{(a,b)} \in \ker\varphi$, alors $g(a)(g(b))^{-1} = 0_{K'}$ d'où $g(a) = 0_{K'}$ et par suite $a = 0_A$, car g est injectif, et $\overline{(a,b)} = \overline{(0,b)} = \overline{(0,1)} = 0_K$. Ainsi $K' \simeq K$ ■

Remarque 3.53

1) Soit $f : A \longrightarrow Fr(A)$ l'homomorphisme injectif défini par $f(a) = \overline{(a,1)}$. Pour tout $x = \overline{(a,b)} \in Fr(A)$, on a $x = \overline{(a,b)} = \overline{(a,1)(1,b)} = f(a)(f(b))^{-1}$ $(= f(a)/f(b))$ d'où l'appellation : corps des fractions de l'anneau intègre A.

2) Puisque $A \simeq f(A)$, on peut identifier l'élément a de A avec son image $f(a) = \overline{(a,1)}$ et remplacer $f(A)$ par A ; on peut alors considérer A comme un sous-anneau de $Fr(A)$ et écrire l'élément $x = \overline{(a,b)} = f(a)(f(b))^{-1}$ de $Fr(A)$ sous la forme $\frac{a}{b}$.

Exemple 3.54 $Fr(\mathbb{Z}) = \mathbb{Q}$.

Chapitre 4

Divisibilité dans les anneaux principaux

Soient A un anneau commutatif (unitaire et non trivial), a et b deux éléments de A. On dit que a **divise** b (ou b est un **multiple** de a) et on note a/b s'il existe un élément c de A tel que $b = ac$. Cette relation de divisibilité est une relation de préordre (i.e., reflexive et transitive) mais, non symétrique.

Proposition 4.1 *Soient a et b deux éléments d'un anneau commutatif A (unitaire et non trivial).*

(i) a/b si, et seulement si, $(b) \subset (a)$.

(ii) $u \in \mathcal{U}(A)$ si, et seulement si, $\forall a \in A$, u/a.

(iii) Les éléments de la forme ua, où $u \in \mathcal{U}(A)$, divisent a.

(iv) Si A est intègre, alors a/b et b/a si, et seulement si, $a = ub$, avec $u \in \mathcal{U}(A)$. Dans ce cas, on dit que a et b sont ***associés*** *et on note* $\mathbf{a} \sim \mathbf{b}$ *(ou $a \approx b$).*

Remarque 4.2 *Si A est intègre, alors la relation $\sim$ est une relation d'équivalence.*

Exemple 4.3

1) Dans $\mathbb{Z}$, $n \sim m$ si, et seulement si, $m = n$ ou $m = -n$.

2) Soit A un anneau intègre. $u \in \mathcal{U}(A)$ si, et seulement si, $u \sim 1_A$.

Dans toute la suite, tous les anneaux considérés sont supposés être intègres.

4.1 Eléments irréductibles et éléments premiers

Définitions 4.4 *Soit p un élément de A.*

(i) On dit que p est ***irréductible*** *si p est non nul, non inversible et les seuls diviseurs de p sont les éléments inversibles et les associés de p ; i.e., $p \neq 0$, $p \notin \mathcal{U}(A)$ et si a/p, alors $a \in \mathcal{U}(A)$ ou $a = up$, avec $u \in \mathcal{U}(A)$.*

(ii) On dit que p est ***premier*** *si p est non nul, non inversible et si p divise un produit de termes, alors p divise l'un des facteurs de ce produit ; i.e., $p \notin \mathcal{U}(A), p \neq 0$ et si p/ab, alors p/a ou p/b.*

Proposition 4.5 *Soit p un élément de A.*

(i) p est premier dans A si, et seulement si, p est non nul et l'idéal (p) est premier.

(ii) p est irréductible dans A si, et seulement si, p est non nul et l'idéal (p) est maximal dans l'ensemble des idéaux principaux de A différents de A.

(iii) Si p est premier, alors p est irréductible.

Preuve.

(i) Supposons que p est premier, alors $(p) \neq (0)$ et $(p) \neq A$ car $p \notin \mathcal{U}(A)$. Soient $a, b \in A$ tels que $ab \in (p)$, alors p/ab donc p/a ou p/b et ainsi $a \in (p)$ ou $b \in (p)$. Réciproquement, supposons que (p) est premier et p est non nul, alors $p \notin \mathcal{U}(A)$ car $(p) \neq A$. Soient $a, b \in A$ tels que p/ab, alors $ab \in (p)$ donc $a \in (p)$ ou $b \in (p)$ et ainsi p/a ou p/b.

(ii) Supposons que p est irréductible, alors p est non nul et $(p) \neq A$ car $p \notin \mathcal{U}(A)$. Soit $I = (a)$ un idéal principal de A différent de A tel que $(p) \subset I$, alors a/p d'où $a = up$, où $u \in \mathcal{U}(A)$ ($a \notin \mathcal{U}(A)$ car $I \neq A$) et par suite $I = (p)$. Réciproquement, supposons que p est non nul et (p) est maximal dans l'ensemble des idéaux principaux de A différents de A. On a $p \notin \mathcal{U}(A)$ car $(p) \neq A$ et si $a \in A$ tel que a/p, alors $(p) \subset (a)$ donc $(a) = A$ ou $(a) = (p)$ et ainsi $a \in \mathcal{U}(A)$ ou $a = up$, avec $u \in \mathcal{U}(A)$.

(iii) Supposons que p est premier, alors p est non nul et non inversible. Soit $a \in A$ tel que a/p, alors $\exists\ b \in A$ tel que $p = ab$. D'où p/ab et ainsi p/a ou p/b. Si p/a (de même pour le cas p/b), alors $\exists\ c \in A : a = pc$ d'où $p = pcb$, ainsi $cb = 1$ (A est intègre), alors $b \in \mathcal{U}(A)$ et par suite $a \sim p$ ■

Exemple 4.6

1) Dans $\mathbb{Z}$, les notions d'éléments premiers et d'éléments irréductibles coincident. Ces éléments irréductibles (premiers) sont les entiers relatifs p tels que $|p|$ est un nombre premier.

2) L'exemple suivant montre qu'en général, un élément irréductible n'est pas nécessairement premier : Soit $A = \mathbb{Z}[i\sqrt{3}] = \{a + ib\sqrt{3}/a, b \in \mathbb{Z}\}$ (noté aussi $\mathbb{Z}[\sqrt{-3}]$). Commençons par déterminer $\mathcal{U}(A)$: soit $x = a + ib\sqrt{3} \in \mathcal{U}(A)$, alors $\exists\ y = c + id\sqrt{3} \in A$ tel que $xy = 1$. En passant aux modules des complexes, on obtient $(a^2 + 3b^2)(c^2 + 3d^2) = 1$, alors $a^2 + 3b^2 = 1$ d'où $a = \pm 1$ et $b = 0$, alors $\mathcal{U}(A) \subset \{-1, 1\}$ et ainsi $\mathcal{U}(A) = \{-1, 1\}$.

2 est un élément irréductible de A. En effet, $2 \notin \mathcal{U}(A)$ et soit $x = a + ib\sqrt{3} \in A$ tel que $x/2$, alors $\exists y = c + id\sqrt{3} \in A$ tel que $2 = xy = (a + ib\sqrt{3})(c + id\sqrt{3})$. En passant aux modules des complexes, on obtient $4 = (a^2 + 3b^2)(c^2 + 3d^2)$. Comme $a^2 + 3b^2$ est toujours différente de 2, $a^2 + 3b^2 = 1$ ou $c^2 + 3d^2 = 1$ d'où $x = \pm 1 \in \mathcal{U}(A)$ ou $y = \pm 1 \in \mathcal{U}(A)$, alors 2 est irréductible dans A.

Cependant, 2 n'est pas premier dans A. En effet, 2 divise $4 = (1 + i\sqrt{3})(1 - i\sqrt{3})$ et 2 ne divise ni $1 + i\sqrt{3}$ ni $1 - i\sqrt{3}$ (car si 2 divise $1 + i\sqrt{3}$, alors 2 divise 1 dans $\mathbb{Z}$, ce qui est faux; de même 2 ne divise pas $1 - i\sqrt{3}$).

Conséquence 4.7 *p est un élément irréductible (resp. premier) d'un anneau intègre A si, et seulement si, $\forall u \in \mathcal{U}(A)$, up est irréductible (resp. premier) dans A (car $(up) = (p)$).*

4.2 P.G.C.D et P.P.C.M

Définition 4.8 *Soient A un anneau (intègre), a et b deux éléments de A. Un élément d de A est appelé **plus grand commun diviseur** (pgcd) de a et b si :*

(i) d/a et d/b

(ii) Si d'/a et d'/b, alors d'/d.

Remarque 4.9

1) En général, deux éléments d'un anneau intègre n'ont pas nécessairement un pgcd. (cf. Exercice 4.12).

2) Si a et b (éléments d'un anneau intègre A) admettent un pgcd, alors ce pgcd est unique à un facteur inversible près. En effet, si d est un pgcd de a et b et $\delta \in A$ tel que $d \sim \delta$, alors δ est aussi un pgcd de a et b (δ/a et δ/b car δ/d et d/a et d/b; si d'/a et d'/b, alors d'/δ, car d'/d et d/δ). D'autre part si d et δ sont des pgcd de a et b, alors d et δ sont associés (car d/δ et δ/d).

Si d est un pgcd de a et b, on note $\mathbf{d} = \mathbf{p}\,\text{gcd}\,(\mathbf{a}, \mathbf{b})$ ou simplement $\mathbf{d} = \mathbf{a} \wedge \mathbf{b}$.

3) Si a, b et c sont des éléments de A, alors $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ (si ces pgcd existent) et ainsi un pgcd des éléments a, b et c, noté $a \wedge b \wedge c$, n'est autre que $(a \wedge b) \wedge c$ (ou $a \wedge (b \wedge c)$). De la même manière, on définit un pgcd d'un nombre fini d'éléments de A.

*4) On dit que deux éléments a et b **sont premiers entre eux** si $p\gcd(a, b) = 1$.*

Définition 4.10 *Un élément m de A est appelé **plus petit commun multiple** de a et b si :*

(i) a/m et b/m

(ii) Si a/m' et b/m', alors m/m'.

*Si m est un **plus petit commun multiple** de a et b, on note $\mathbf{m} = \mathbf{ppcm(a, b)}$ ou simplement $\mathbf{m} = \mathbf{a} \vee \mathbf{b}$.*

Exercice 4.11 *Soient A un anneau intègre, $a, b \in A$ tels que a et b admettent un ppcm, noté m, et $m' \in A$. Montrer que m' est un ppcm de a et b si, et seulement si, $m \sim m'$.*

Exercice 4.12

1) Soient $a, b \in A - \{0\}$. Montrer que si a et b possèdent un ppcm, noté m, dans A, alors il existe $d \in A : ab = md$ et que $d = a \wedge b$.

2) Soit l'anneau $\mathbb{Z}[i\sqrt{5}] = \{a + ib\sqrt{5}/a, b \in \mathbb{Z}\}$.

a) Déterminer $\mathcal{U}(\mathbb{Z}[i\sqrt{5}])$.

b) Déterminer tous les diviseurs de 9 et de $3(2 + i\sqrt{5})$.

c) Montrer que 1 est un pgcd de 3 et $2+i\sqrt{5}$ et que 3 et $2+i\sqrt{5}$ n'ont pas de ppcm. Conclure.

d) Montrer que les éléments 9 et $3(2 + i\sqrt{5})$ n'ont pas de pgcd dans $\mathbb{Z}[i\sqrt{5}]$.

4.3 Divisibilité dans un anneau principal

Dans toute la suite, nous supposons que A est un anneau principal.

Proposition 4.13

(i) Tout élément irréductible de A est premier.

(ii) Tout idéal premier non nul de A est maximal.

Preuve.

(i) Soit $p \in A$ irréductible dans A, alors $p \neq 0$ et $p \notin \mathcal{U}(A)$. D'après la proposition 4.5 (ii), l'idéal (p) de A est un idéal maximal de A (car tous les idéaux de A sont principaux), d'où (p) est un idéal premier non nul et ainsi, d'après la proposition 4.5 i), p est premier.

(ii) Soit I un idéal premier non nul de A. Alors $I = (a)$ avec $a \in A$ (A est principal) et d'après la proposition 4.5 i), a est premier et aussi d'après (iii) de la même proposition, a est irréductible. D'autre part, puisque tous les idéaux de A sont principaux (A est principal) et en utilisant (ii) de la proposition 4.5, $I = (a)$ est un idéal maximal de A ■

Remarque 4.14 *Dans un anneau principal, les notions d'éléments premiers et d'éléments irréductibles coincident. (cf. proposition précédente et proposition 4.5).*

Proposition 4.15 *Soient a et b deux éléments de A. Alors a et b admettent un pgcd et un ppcm et :*

(i) $a \wedge b = d$ si, et seulement si, $(a) + (b) = (d)$.

(ii) $a \vee b = m$ si, et seulement si, $(a) \cap (b) = (m)$.

Preuve.

Soient a et b deux éléments de A. Puisque A est principal, l'idéal (a)+(b) est principal et ainsi $\exists d \in A : (a) + (b) = (d)$. On a $d = p\gcd(a, b)$. En effet, d/a (car $(a) \subset (a) + (b) = (d)$) et d/b (car

$(b) \subset (a)+(b) = (d)$). D'autre part, si c/a et c/b, alors $(a) \subset (c)$ et $(b) \subset (c)$ d'où $(d) = (a)+(b) \subset (c)$, alors c/d. Ainsi, si $(a) + (b) = (d)$, d est un pgcd de a et b.

Réciproquement, si $a \wedge b = d$, alors $(a) \subset (d)$ (car d/a) et $(b) \subset (d)$ (car d/b), d'où $(a)+(b) \subset (d)$. D'autre part, l'idéal $(a) + (b)$ est un idéal principal (A est principal) d'où $\exists\ c \in A$ tel que $I = (a) + (b) = (c)$, alors c/a (car $(a) \subset (a) + (b) = (c)$) et c/b (car $(b) \subset (a) + (b) = (c)$) d'où, par définition de d, c/d et ainsi $(d) \subset (c) = (a) + (b)$.

De même, on montre l'existence du *ppcm* et (ii) ∎

Théorème 4.16 (Théorème de Bezout) *Soient a et b deux éléments de A. a et b sont premiers entre eux si, et seulement si, il existe u et v, deux éléments de A, tels que $au + bv = 1$.*

Preuve. En utilisant la proposition précédente, a et b sont premiers entre eux si, et seulement si, $(a) + (b) = (1) = A$ si, et seulement si, $\exists\ u, v \in A : 1 = ua + vb$ ∎

Proposition 4.17 *Soient a, b et c des éléments non nuls de A.*
(i) Si $a \wedge b = 1$ et $a \wedge c = 1$, alors $a \wedge bc = 1$.
(ii) Si a/bc et $a \wedge b = 1$, alors a/c (Théorème de Gauss).
(iii) Si b/a et c/a et $b \wedge c = 1$, alors bc/a.

Preuve. (iii) découle immédiatement de l'exercice 4.12.

Montrons par exemple (ii). Puisque $a \wedge b = 1$, $\exists u, v \in A : ua + vb = 1$. En multipliant les deux membres de cette égalité par c, on obtient $c = uac + v(bc)$ et comme $bc = ad$, où $d \in A$, on a $c = a(uc + vd)$ et ainsi a/c ∎

Théorème 4.18
(i) Tout élément non nul et non inversible a de A s'écrit sous la forme $a = p_1...p_r$, où $p_1, ..., p_r$ sont des éléments irréductibles de A non nécessairement distincts.
(ii) Si un élément non nul et non inversible a de A possède une autre décomposition de type $a = q_1...q_s$ où $q_1, ..., q_s$ sont des éléments irréductibles de A, alors $r = s$ et il existe une permutation σ de S_r telle que p_i et $q_{\sigma(i)}$ sont associés pour tout $i \in \{1, ..., r\}$.

Preuve.

Montrons d'abord que A vérifie la condition de chaine ascendante pour les idéaux, i.e., si $a_1, a_2, ...$ sont des éléments de A tels que $(a_1) \subset (a_2) \subset \dots$ (les idéaux de A sont principaux), alors $\exists\ n \in \mathbb{N}^*$ tel que $(a_n) = (a_{n+1}) = (a_{n+m})\ \forall m \in \mathbb{N}$. Soit $I = \bigcup_{i \geq 1} (a_i)$. On vérifie facilement que I est un idéal de A, alors $I = (a)$ (car A est principal). Comme $a \in I$, $\exists n \geq 1$ tel que $a \in (a_n)$ d'où $(a) \subset (a_n)$. D'autre part, $(a_n) \subset I = (a)$ et ainsi $I = (a) = (a_n)$. On a aussi $\forall m \in \mathbb{N}$, $I = (a_n) \subset (a_{n+m}) \subset I = (a) = (a_n)$ donc $(a_n) = (a_{n+m})$, i.e., la suite $(a_i)_{i \geq 1}$ est stationnaire à partir du rang n.

Supposons que A ne vérifie pas la condition (i). Alors il existe $a_1 \in A - \{0\}$ non inversible tel que a_1 ne s'écrit pas sous la forme indiquée dans la condition (i). a_1 n'est pas irréductible d'où $a_1 = a_2 b_2$, où $a_2, b_2 \notin \mathcal{U}(A)$ et l'un au moins des éléments a_2 et b_2 n'est pas irréductible (si a_2 et b_2 sont irréductibles alors $a_1 = a_2 b_2$ vérifie (i)). Supposons que a_2 est non irréductible, alors $(a_1) \subsetneq (a_2)$ (l'inclusion est stricte car si $a_2 = c_1 a_1$, on aura $a_1 = c_1 a_1 b_2$ d'où $b_2 \in \mathcal{U}(A)$) et $a_2 = a_3 b_3$ où $a_3, b_3 \notin \mathcal{U}(A)$. L'un au moins des éléments a_3 et b_3 n'est pas irréductible (dans le cas où a_3 et b_3 sont irréductibles, b_2 n'est pas irréductible, sinon $a_1 = a_2 b_2 = a_3 b_3 b_2$ vérifie (i) et, dans ce cas, on prend b_2 au lieu de a_2). Si a_3 est non irréductible, alors on a $(a_1) \subsetneq (a_2) \subsetneq (a_3)$ et $a_3 = a_4 b_4$ où $a_4, b_4 \notin \mathcal{U}(A)$ et on a $(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq (a_4)$. De proche en proche, on construit une suite croissante d'idéaux $((a_i))_{i \geq 1}$ non stationnaire ce qui contredit le fait que A vérifie la condition de chaine ascendante.

Montrons que A vérifie la condition (ii) : Soit $a = p_1 \dots p_r = q_1 \dots q_s$, où $p_1, \dots, p_r, q_1, \dots, q_s$ sont des irréductibles. $p_1 / q_1 \dots q_s$ et p_1 est premier (car p_1 est irréductible et A est principal), d'où $\exists i$ tel

que p_1/q_i donc p_1 et q_i sont associés, alors $\exists u_1 \in \mathcal{U}(A)/\ q_i = u_1 p_1$. Posons $q_i = q_1$ (quitte à changer la numérotation), ainsi $p_2 \dots p_r = u_1 q_2 \dots q_s$. En reprenant le même raisonnement pour p_2, on obtient $p_3 \dots p_r = u_1 u_2 q_3 \dots q_s$. Ceci prouve que $r = s$ et que p_i et q_j sont associés deux à deux ■

Remarque 4.19 *Un anneau intègre vérifiant (i) et (ii) est appelé anneau* ***factoriel****. Ainsi, un anneau principal est factoriel.*

Soient A un anneau principal, a et b deux éléments non nuls et non inversibles de A. On note $\mathcal{P}$ un ensemble d'éléments irréductibles de A tel que si p est irréductible dans A, alors p est associé à un, et un seul, élément de $\mathcal{P}$. Comme A est principal, a et b se décomposent en produit d'éléments de $\mathcal{P}$: $a = p_1^{\alpha_1} ... p_r^{\alpha_r}$ et $b = p_1^{\beta_1} ... p_r^{\beta_r}$ où $p_i \in \mathcal{P}, p_i \neq p_j$ si $i \neq j, \alpha_i \geq 0, \beta_i \geq 0$ (les décompositions de a et b contiennent les mêmes éléments de $\mathcal{P}$ quitte à ce que certains d'entre eux aient des exposants nuls).

Théorème 4.20 *Avec les notations ci-dessus,*
(i) a/b si, et seulement si, $\alpha_i \leq \beta_i$ pour tout $i \in \{1, ..., r\}$.
(ii) $a \wedge b = p_1^{\lambda_1} ... p_r^{\lambda_r}$, où $\lambda_i = \min\{\alpha_i, \beta_i\}$ pour tout $i \in \{1, ..., r\}$.
(iii) $a \vee b = p_1^{\mu_1} ... p_r^{\mu_r}$, où $\mu_i = \max\{\alpha_i, \beta_i\}$ pour tout $i \in \{1, ..., r\}$.

Preuve. (i) Il est évident que si $\alpha_i \leq \beta_i$ pour tout $i \in \{1, ..., r\}$ alors a/b.
Réciproquement, supposons que a/b, alors $b = ac$. On distingue les deux cas suivants :
- $c \in \mathcal{U}(A)$, alors, en utilisant la définition de $\mathcal{P}$, $c = 1$ et ainsi $\alpha_i = \beta_i$
- $c \notin \mathcal{U}(A)$, d'où c se décompose en produit d'éléments de $\mathcal{P}$ et puisque $b = ac$, alors $\alpha_i \leq \beta_i$ pour tout $i \in \{1, ..., r\}$.
Les assertions (ii) et (iii) découlent de (i) ■

Remarque 4.21 *Si $a = 0$ (resp. $b = 0$), alors b (resp. a) est un pgcd de a et b . Aussi, si $a \in \mathcal{U}(A)$ ou $b \in \mathcal{U}(A)$), alors 1 est un pgcd de a et b.*

Chapitre 5

Anneau de Polynômes à une Indéterminée

Dans toute la suite, A désigne un anneau commutatif (unitaire et non trivial).

5.1 Construction

5.1.1 Construction et Définitions

Définitions 5.1 - *On appelle* ***polynôme à une indéterminée à coefficients dans l'anneau A*** *toute suite $(a_n)_{n\in\mathbb{N}}$ d'éléments de A n'ayant qu'un nombre fini de termes non nuls.*

- Les éléments a_i non nuls de cette suite sont appelés les ***coefficients*** *du polynôme $(a_n)_{n\in\mathbb{N}}$.*

- Le coefficient non nul correspondant à l'indice le plus grand de cette suite est appelé ***coefficient dominant*** *du polynôme $(a_n)_{n\in\mathbb{N}}$.*

- Le coefficient a_0 est dit ***coefficient constant*** *du polynôme $(a_n)_{n\in\mathbb{N}}$.*

- Si le coefficient dominant du polynôme $(a_n)_{n\in\mathbb{N}}$ est égal à 1, on dit que $(a_n)_{n\in\mathbb{N}}$ est un ***polynôme unitaire****.*

Exemple 5.2 *Soit $(a_n)_{n\in\mathbb{N}} = (1, 0, -2, 1, 0, ..., 0, ...)$ la suite d'éléments de $\mathbb{Z}$ définie par : $a_0 = 1, a_1 = 0, a_2 = -2, a_3 = 1$ et $a_n = 0$ si $n \geq 4$. La suite $(a_n)_{n\in\mathbb{N}}$ est un polynôme à une indéterminée à coefficients dans l'anneau $\mathbb{Z}$. Les éléments $a_0 = 1, a_1 = 0, a_2 = -2, a_3 = 1$ sont les coefficients du polynôme $(a_n)_{n\in\mathbb{N}}$; $a_0 = 1$ est le coefficient constant de $(a_n)_{n\in\mathbb{N}}$, $a_3 = 1$ est le coefficient dominant de $(a_n)_{n\in\mathbb{N}}$ et le polynôme $(a_n)_{n\in\mathbb{N}}$ est unitaire ($a_3 = 1$).*

On définit dans l'ensemble B des polynômes à une indéterminée à coefficients dans l'anneau A les deux opérations suivantes :

- Addition : $\forall P = (a_n)_{n\in\mathbb{N}} \in B$, $\forall Q = (b_n)_{n\in\mathbb{N}} \in B : P + Q = (c_n)_{n\in\mathbb{N}}$ est la suite d'éléments de A définie par la relation : $c_n = a_n + b_n$; $P + Q \in B$ car $P + Q = (c_n)_{n\in\mathbb{N}}$ est une suite n'ayant qu'un nombre fini de termes non nuls.

- Produit : $\forall P = (a_n)_{n\in\mathbb{N}} \in B$, $\forall Q = (b_n)_{n\in\mathbb{N}} \in B : P.Q = (c_n)_{n\in\mathbb{N}}$ avec : $c_n = \sum_{i+j=n} a_i b_j$ ainsi $c_0 = a_0b_0, c_1 = a_0b_1 + a_1b_0, ..., c_k = a_0b_k + a_1b_{k-1} + ... + a_{k-1}b_1 + a_kb_0, ...$ et si $a_i = 0$ $\forall i > n_1$ et $b_j = 0$ $\forall j > m_1$, alors $c_k = 0$ $\forall k > n_1 + m_1$ et ainsi $P.Q = (c_n)_{n\in\mathbb{N}}$ est une suite n'ayant qu'un nombre fini de termes non nuls, i.e., $PQ \in B$.

On vérifie aisément que l'ensemble B des polynômes à une indéterminée à coefficients dans A, muni de l'addition et de la multiplication définies ci-dessus, est un anneau commutatif unitaire (et non trivial) appelé **anneau de polynômes à une indéterminée à coefficients dans l'anneau A**. Le zéro de B est l'élément $(0_A, 0_A, ...)$ et son unité est l'élément $(1_A, 0_A, 0_A, ...)$.

A l'aide de l'homomorphisme injectif $\mathfrak{i} : A \longrightarrow B$ défini par $\mathfrak{i}(a) = (a, 0, 0, ...)$, on peut identifier a avec son image $\mathfrak{i}(a)$, A avec $\mathfrak{i}(A)$ et considérer A comme un sous-anneau de B. Les éléments de A s'appellent **polynômes constants**.

Notation 5.3 (Notations habituelles)
- Posons $X = (0, 1, 0, 0, ...) \in B$. *On a* $X^2 = X.X = (0, 0, 1, 0, 0, ...), \dots, X^k = (\underbrace{0, ..., 0}_{k\ fois}, 1, 0, 0, ...)$ *et ainsi* $(0, ..., 0, a_k, 0, ...) = (a_k, 0, ...)(0, ..., 0, 1, 0, ...) = (a_k, 0, ...)X^k$.

Soit $P = (a_0, a_1, ..., a_n, 0, 0, ...)$ *un élément de B. En utilisant l'identification de a avec son image* $\mathfrak{i}(a) = (a, 0, 0, ...)$, *on a* $P = (a_0, 0, ...) + (0, a_1, 0, ...) + ... + (0, ..., 0, a_n, 0, ...) = a_0 + a_1X + ... + a_nX^n$. *Ainsi* $P(X) = a_0 + a_1X + ... + a_nX^n = 0$ *si, et seulement si,* $a_0 = ... = a_n = 0$.

- Vu la notation utilisée ci-dessus, on désigne l'anneau B par $\mathbf{A[X]}$.

Dans tout ce qui suit, nous n'allons adopter que ces notations.

Définition 5.4 *Soit* $P(X) = \sum_{i=0}^{n} a_iX^i = a_0 + a_1X + ... + a_nX^n$ *un polynôme non nul de* $A[X]$. *On appelle* ***degré du polynôme*** *P, noté* ***degP****, le plus grand entier k tel que* a_k *est non nul.*

Ainsi $\deg P = 0$ *si, et seulement si, P est un polynôme constant non nul.*

Si P est le polynôme nul, on pose $\deg P = -\infty$ *et on convient que* $\forall n \in \mathbb{N}$, $-\infty \leq n$ *et que* $-\infty + n = -\infty$.

5.1.2 Propriétés

Proposition 5.5 *Si P et Q sont des polynômes de* $A[X]$, *alors*
(i) $\deg(P + Q) \leq \sup(\deg P, \deg Q)$.
(ii) $\deg(P.Q) \leq \deg P + \deg Q$.
(iii) $\mathcal{U}(A) \subset \mathcal{U}(A[X])$, *où* $\mathcal{U}(A[X])$ *désigne le groupe des éléments inversibles de* $A[X]$.

Remarque 5.6 *L'inégalité (ii) peut être stricte ainsi que l'inclusion (iii). En effet, considérons* $P = \overline{2}X, Q = \overline{2}X + \overline{1} \in (\mathbb{Z}/4\mathbb{Z})[X]$. *On a* $P.Q = \overline{2}X$ *et ainsi* $\deg PQ < \deg P + \deg Q$. *On voit aussi que Q est inversible dans* $(\mathbb{Z}/4\mathbb{Z})[X]$ $((\overline{1} + \overline{2}X)(\overline{1} + \overline{2}X) = \overline{1})$ *et ainsi* $\mathcal{U}(\mathbb{Z}/4\mathbb{Z}) \subsetneq \mathcal{U}((\mathbb{Z}/4\mathbb{Z})[X])$.

Proposition 5.7 *Si A est intègre, alors*
(i) $A[X]$ *est un anneau intègre (en particulier, si* $A = K$ *est un corps, alors* $K[X]$ *est intègre).*
(ii) $\deg(P.Q) = \deg P + \deg Q$, $\forall P, Q \in A[X]$ *(en particulier, si* $A = K$ *est un corps).*
(iii) $\mathcal{U}(A[X]) = \mathcal{U}(A)$ *(en particulier si* $A = K$ *est un corps, alors* $\mathcal{U}(K[X]) = K^* = K - \{0\}$).

Preuve. Montrons par exemple (ii). Si $P = 0$ ou $Q = 0$ alors (ii) est évidente. Supposons alors que $P \neq 0$, $Q \neq 0$ et notons $\deg P = n$ et $\deg Q = m$. Posons $P = a_0 + a_1X + \dots + a_nX^n$ et $Q = b_0 + b_1X + \dots + b_mX^m$, alors $PQ = \sum_{k=0}^{n+m} c_kX^k$ et $c_{n+m} = a_nb_m \neq 0$ car $a_n \neq 0$ et $b_m \neq 0$ et A est intègre ■

5.2 Division euclidienne

Théorème 5.8 (Théorème de la division euclidienne) *Soient P et S des polynômes de* $A[X]$ *tels que S est non nul et le coefficient dominant de S est inversible dans A, alors il existe un, et un seul, couple* (Q, R) *élément de* $(A[X])^2$ *tel que* $P = SQ + R$ *avec* $\deg R < \deg S$.

En particulier, si $A = K$ *est un corps (commutatif) et* $(P, S) \in K[X] \times (K[X] - \{0\})$, *alors il existe un, et un seul, couple* $(Q, R) \in (K[X])^2$ *tel que* $P = SQ + R$ *avec* $\deg R < \deg S$.

Preuve.

Existence :

- Si $degP < degS$, on pose $Q = 0$ et $R = P$, alors $P = QS + R$ et $\deg R < \deg S$.

- Si $degP = n \geq \deg S = m$, utilisons une récurrence sur n :

* Si $n = 0$, alors $m = 0$ d'où $P = a \in A$ et $S = b \in \mathcal{U}(A)$. Si on pose $Q = (b^{-1}a)$ et $R = 0$, alors $P = QS + R$ avec $\deg R < \deg S$.

* Supposons que ce résultat est vrai pour tous les polynômes de degré $< n$.

* Soient P=$\sum_{i=0}^{n} a_i X^i$ un polynôme de degré n et $S = \sum_{i=0}^{m} b_i X^i$ un polynôme de degré m avec $b_m \in \mathcal{U}(A)$. Posons $T = b_m P - a_n X^{n-m} S$, alors $\deg T < n$ et ainsi $\exists Q_1, R_1 \in A[X]$ tels que $b_m P - a_n X^{n-m} S = T = Q_1 S + R_1$ avec $\deg R_1 < \deg S$ donc $b_m P = (Q_1 + a_n X^{n-m})S + R_1$ et comme $b_m \in \mathcal{U}(A)$, alors $P = QS + R$ avec $Q = b_m^{-1}(Q_1 + a_n X^{n-m})$, $R = b_m^{-1} R_1$ et $\deg R < \deg S$.

Unicité :

Si $P = Q_1 S + R_1$ avec $\deg R_1 < \deg S$ et $P = Q_2 S + R_2$ avec $\deg R_2 < \deg S$, alors $(Q_1 - Q_2)S = R_2 - R_1$ d'où nécessairement $Q_1 - Q_2 = 0$ (si $Q_1 - Q_2 \neq 0$, alors, puisque le coefficient dominant de S est inversible dans A, $\deg(Q_1 - Q_2)S \geq \deg S$. Or, $\deg(R_2 - R_1) \leq \sup(\deg R_1, \deg R_2) < \deg S$) alors $R_2 - R_1 = 0$ et ainsi $Q_1 = Q_2$ et $R_1 = R_2$ ■

Exemple 5.9

1) Soient $P = X^4 + \overline{3}X^3 + \overline{2}X, S = \overline{3}X^3 + \overline{1} \in \mathbb{Z}/4\mathbb{Z}[X]$. Puisque $\overline{3} \in \mathcal{U}(\mathbb{Z}/4\mathbb{Z})$, il existe un unique couple $(Q, R) \in (\mathbb{Z}/4\mathbb{Z}[X])^2$ tel que $P = QS + R$ avec $\deg R < \deg S$ ($Q = \overline{3}X + \overline{1}$ et $R = \overline{3}X + \overline{3}$).

2) Dans $\mathbb{Z}/4\mathbb{Z}[X]$, on ne peut pas trouver $(Q, R) \in (\mathbb{Z}/4\mathbb{Z}[X])^2$ tel que $X^3 + \overline{1} = Q.(\overline{2}X) + R$ avec $\deg R < 1$. En effet, supposons qu'il existe $(Q, R) \in (\mathbb{Z}/4\mathbb{Z}[X])^2$ tel que $X^3 + \overline{1} = Q.(\overline{2}X) + R$ avec $\deg R < 1$, alors, en posant $R = \bar{a} \in \mathbb{Z}/4\mathbb{Z}$ et après identification, on a $\overline{2} \in \mathcal{U}(\mathbb{Z}/4\mathbb{Z})$, ce qui est faux.

5.3 Fonctions polynômes

5.3.1 Définition et Théorème du reste

Soient $(\mathcal{A}(A, A), +, .)$ l'anneau des applications de A dans A (cf. chapitre 3, exemple 3.3, 7)) et $P = \sum_{i=0}^{n} a_i X^i \in A[X]$. On considère l'application notée $\tilde{P} : A \longrightarrow A, \alpha \longmapsto \tilde{P}(\alpha) = \sum_{i=0}^{n} a_i \alpha^i$.
L'application $\tilde{P}$ est appelée **fonction polynôme associée au polynôme P**.

Soit $\varphi : A[X] \longrightarrow \mathcal{A}(A, A)$ l'application définie par $\varphi(P) = \tilde{P}$. On vérifie facilement que φ est un homomorohisme d'anneaux.

Théorème 5.10 (Théorème du reste) *Soient P un polynôme de $A[X]$ et α un élément de A, alors il existe un unique polynôme $Q \in A[X]$ tel que $P(X) = Q(X)(X - \alpha) + \tilde{P}(\alpha)$.*

Preuve. Puisque le coefficient dominant de $X - \alpha$ est égal à 1, alors on peut effectuer la division euclidienne de P par $X - \alpha$ d'où il existe un unique couple (Q, R) élément de $(A[X])^2$ tel que : $P = Q(X - \alpha) + R$ avec $\deg R < 1$, i.e., $R = c \in A$ et on a : $\tilde{P}(\alpha) = c$ ■

5.3.2 Racine d'un polynôme

Définition 5.11 *Soient $P \in A[X]$ et $\alpha \in A$. On dit que α est une **racine** (ou un zéro) de P si $\tilde{P}(\alpha) = 0$.*

Proposition 5.12 *Soient $P \in A[X]$ et $\alpha \in A$. α est une racine de P si, et seulement si, $(X - \alpha)$ divise P.*

Preuve. Supposons que α est une racine de P, alors, d'après le théorème du reste, $P(X) = Q(X)(X-\alpha) + \tilde{P}(\alpha) = Q(X)(X-\alpha)$ et ainsi $(X-\alpha)/P$. Réciproquement, supposons que $(X-\alpha)/P$, alors $P(X) = Q(X)(X-\alpha)$ avec $Q \in A[X]$ et ainsi $\tilde{P}(\alpha) = \tilde{Q}(\alpha)(\alpha-\alpha) = 0$ ■

Proposition 5.13 *Si A est intègre et $P \in A[X]$ un polynôme non nul de degré n, alors le polynôme P a au plus n racines distinctes.*

Preuve. - Montrons d'abord, par récurrence sur m, que si $\alpha_1, ...$ et α_m sont des racines distinctes de P, alors $(X-\alpha_1)...(X-\alpha_m)/P$

* Si $m = 1$ et α_1 une racine de P, alors $(X-\alpha_1)/P$ (cf. la proposition 5.12).

* Supposons que ce résultat est vrai pour m.

* Soient $P \in A[X]$, $\alpha_1, ...$ et α_{m+1} des racines distinctes de P. En utilisant l'hypothèse de récurrence, $(X-\alpha_1)...(X-\alpha_m)/P$, i.e., $\exists Q \in A[X] : P = (X-\alpha_1)...(X-\alpha_m)Q$. On a aussi $\tilde{P}(\alpha_{m+1}) = (\alpha_{m+1}-\alpha_1)...(\alpha_{m+1}-\alpha_m)\tilde{Q}(\alpha_{m+1}) = 0$ et puisque $\alpha_{m+1} - \alpha_i \neq 0\ \forall i = 1, ..., m$ et A est intègre, alors $(\alpha_{m+1}-\alpha_1)...(\alpha_{m+1}-\alpha_m) \neq 0$ et ainsi $\tilde{Q}(\alpha_{m+1}) = 0$ d'où $Q = (X-\alpha_{m+1})S$ avec $S \in A[X]$ donc $P = (X-\alpha_1)...(X-\alpha_m)(X-\alpha_{m+1})S$.

- Supposons que $\alpha_1, ...$ et α_m sont des racines distinctes de P et que $m > n$, alors $(X-\alpha_1)...(X-\alpha_m)/P$ d'où $\exists Q \in A[X] : P = (X-\alpha_1)...(X-\alpha_m)Q$ ainsi $n = \deg P = m + \deg Q$ ce qui contredit le fait que $m > n$ ■

Corollaire 5.14 *Si A est un anneau intègre et infini, alors l'homomorphisme d'anneaux $\varphi : A[X] \longrightarrow \mathcal{A}(A, A)$, défini par $\varphi(P) = \tilde{P}$, est un homomorphisme injectif.*

Remarque 5.15

1) Le résultat de la proposition 5.13 est faux si A n'est pas intègre. En effet, $P(X) = \bar{2}X \in (\mathbb{Z}/4\mathbb{Z})[X]$ est un polynôme de degré 1 ayant 2 racines ($\tilde{P}(\bar{0}) = \tilde{P}(\bar{2}) = \bar{0}$).

2) En général et même si A est un corps, on peut avoir $\tilde{P} = 0$ sans que P soit nul, (i.e., on peut avoir φ non injectif). En effet, soit $P = X^p - X \in (\mathbb{Z}/p\mathbb{Z})[X]$, où p est un nombre premier. On a $P \neq 0$, cependant, $\forall \overline{a} \in \mathbb{Z}/p\mathbb{Z} : \tilde{P}(\overline{a}) = \overline{a}^p - \overline{a} = \overline{0}$ (Petit théorème de Fermat) et ainsi $\tilde{P}$ est nulle.

5.4 Polynôme dérivé

Soit K un corps (commutatif).

Définition 5.16 *Soit $P = a_0 + a_1X + a_2X^2 + ... + a_nX^n$ un polynôme de $K[X]$. On appelle **polynôme dérivé** de P le polynôme $P^{'} = a_1 + 2a_2X + ... + na_nX^{n-1}$*

Proposition 5.17 *Si P, Q sont deux polynômes de $K[X]$ et $a \in A$, alors*

1) $(P+Q)^{'} = P^{'} + Q^{'}$

2) $(PQ)^{'} = P^{'}Q + PQ^{'}$

3) $(aP)^{'} = aP^{'}$

Remarque 5.18 *Soit K un corps de caracéristique nulle. Si Le polynôme dérivé $P^{'}$ d'un polynôme $P \in K[X]$ est nul, alors P est un polynôme constant. Cependant, ce résultat est faux si $carK = p \neq 0$ (exemple : $P = X^p \in (\mathbb{Z}/p\mathbb{Z})[X]$, où p est premier, $P' = pX^{p-1} = 0$).*

On définit le polynôme dérivé $P^{(k)}$ d'ordre k de P comme suit : $P^{(0)} = P$, $P^{(1)} = P^{'}$ et $P^{(k+1)} = (P^{(k)})^{'}$ pour $k \geq 2$.

Proposition 5.19 (Formule de Leibnitz) *Soient K un corps, P et Q deux élements de $K[X]$, alors $(P.Q)^{(k)} = \sum_{i=0}^{k} C_k^i P^{(i)} Q^{(k-i)}$ pour tout entier naturel k.*

Preuve. Utilisons une récurrence sur k :

* Pour $k = 0$ et $k = 1$, le résultat est trivial.

* Supposons que le résultat est vrai pour k.

* Pour $k+1$: $(P.Q)^{(k+1)} = ((P.Q)^{(k)})' = (\sum_{i=0}^{k} C_k^i P^{(i)} Q^{(k-i)})' = \sum_{i=0}^{k} C_k^i (P^{(i)} Q^{(k-i)})'$

$$= \sum_{i=0}^{k} C_k^i ((P^{(i)})' Q^{(k-i)} + P^{(i)} (Q^{(k-i)})') = \sum_{i=0}^{k} C_k^i (P^{(i+1)} Q^{(k-i)} + P^{(i)} Q^{(k+1-i)})$$

$$= \sum_{i=0}^{k} C_k^i P^{(i+1)} Q^{(k-i)} + \sum_{i=0}^{k} C_k^i P^{(i)} Q^{(k+1-i)} = \sum_{j=1}^{k+1} C_k^{j-1} P^{(j)} Q^{(k+1-j)} + \sum_{i=0}^{k} C_k^i P^{(i)} Q^{(k+1-i)}$$

$$= \sum_{i=0}^{k+1} C_k^{i-1} P^{(i)} Q^{(k+1-i)} + \sum_{i=0}^{k+1} C_k^i P^{(i)} Q^{(k+1-i)} = \sum_{i=0}^{k+1} (C_k^{i-1} + C_k^i) P^{(i)} Q^{(k+1-i)}$$

$$= \sum_{i=0}^{k+1} C_{k+1}^i P^{(i)} Q^{(k+1-i)} \text{ (car } C_k^{i-1} + C_k^i = C_{k+1}^i) \quad \blacksquare$$

Théorème 5.20 (Formule de Taylor) *Soit K un corps de caractéristique nulle.*

Si $P \in K[X]$ est de degré n et α est un élément de K, alors $P(X) = \sum_{k=0}^{n} \frac{\widetilde{P^{(k)}}(\alpha)}{k!} (X-\alpha)^k$ et ainsi $(X-\alpha)^m$ divise P si, et seulement si, $\tilde{P}(\alpha) = ... = \widetilde{P^{(m-1)}}(\alpha) = 0$.

Preuve.

- Vu la linéarité de la dérivation, il suffit de montrer la formule de Taylor pour le polynôme $Q(X) = X^r$. On a $X^r = ((X-\alpha)+\alpha)^r = \sum_{k=0}^{r} C_r^k (X-\alpha)^k \alpha^{r-k}$. D'autre part, on a $Q^{'}(X) = rX^{r-1}$ et $Q^{(k)}(X) = r(r-1)...(r-k+1)X^{r-k} = k! C_r^k X^{r-k}$ d'où $\widetilde{Q^{(k)}}(\alpha) = k! C_r^k \alpha^{r-k}$. Puisque $car K = 0$, alors $k!.1_K$ est inversible dans K et ainsi $C_r^k \alpha^{r-k} = \frac{\widetilde{Q^{(k)}}(\alpha)}{k!}$, alors $Q(X) = \sum_{k=0}^{r} \frac{\widetilde{Q^{(k)}}(\alpha)}{k!} (X-\alpha)^k$.

- Soit $m \leq n$, alors, d'après la formule de Taylor, $P(X) = \sum_{k=0}^{m-1} \frac{\widetilde{P^{(k)}}(\alpha)}{k!} (X-\alpha)^k + (X-\alpha)^m Q(X)$, où $Q(X) = \sum_{k=0}^{n-m} \frac{\widetilde{P^{(m+k)}}(\alpha)}{(m+k)!} (X-\alpha)^k \in K[X]$. On a $\deg(\sum_{k=0}^{m-1} \frac{\widetilde{P^{(k)}}(\alpha)}{k!} (X-\alpha)^k) < m$ ainsi $Q(X)$ et $R(X) = \sum_{k=0}^{m-1} \frac{\widetilde{P^{(k)}}(\alpha)}{k!} (X-\alpha)^k$ sont respectivement le quotient et le reste de la division euclidienne de $P(X)$ par $(X-\alpha)^m$ dans $K[X]$, alors $(X-\alpha)^m / P(X)$ si, et seulement si, $R(X) = \sum_{k=0}^{m-1} \frac{\widetilde{P^{(k)}}(\alpha)}{k!} (X-\alpha)^k = 0$, i.e., si, et seulement si, $\tilde{P}(\alpha) = ... = \widetilde{P^{(m-1)}}(\alpha) = 0$ $\blacksquare$

Définition 5.21 *Soient $P \in A[X]$, $\alpha \in A$ et $m \in \mathbb{N}^*$. On dit que α est une racine de P d'ordre de multiplicité m si $(X-\alpha)^m$ divise P et $(X-\alpha)^{m+1}$ ne divise pas P.*

Théorème 5.22 *Soient $P \in A[X]$, $\alpha \in A$ et $m \in \mathbb{N}^*$. Les deux propositions suivantes sont équivalentes :*

(i) α est une racine de P d'ordre de multiplicité m.

(ii) Il existe un polynôme $Q \in A[X]$ tel que $P = (X-\alpha)^m Q$ et $\tilde{Q}(\alpha) \neq 0$.

Ainsi, si K est un corps de caractéristique nulle, $P \in K[X]$ de degré n et α un élément de K. Alors α est une racine de P d'ordre de multiplicité égale à un entier $m > 0$ si, et seulement si, $\tilde{P}(\alpha) = ... = \widetilde{P^{(m-1)}}(\alpha) = 0$ et $\widetilde{P^{(m)}}(\alpha) \neq 0$.

Preuve. Montrons que les propriétés (i) et (ii) sont équivalentes. Supposons que α est une racine de P d'ordre de multiplicité m, i.e., $(X-\alpha)^m$ divise P et $(X-\alpha)^{m+1}$ ne divise pas P d'où il existe un polynôme $Q \in A[X]$ tel que $P = (X-\alpha)^m Q$. Alors, $\tilde{Q}(\alpha) \neq 0$ car si $\tilde{Q}(\alpha) = 0$, $X - \alpha / Q$ et par conséquent $(X-\alpha)^{m+1}/P$. Réciproquement, supposons qu'il existe un polynôme $Q \in A[X]$ tel que $P = (X-\alpha)^m Q$ et $\tilde{Q}(\alpha) \neq 0$. Effectuons la division euclidienne de Q par $X - \alpha$ alors $\exists!(Q_1, R_1) \in (A[X])^2 : Q = (X-\alpha)Q_1 + R_1$ ($R_1 = \tilde{Q}(\alpha) \neq 0$) d'où $P = (X-\alpha)^{m+1}Q_1 + R_1(X-\alpha)^m$ alors Q_1 et $R_1(X-\alpha)^m$ sont respectivement le quotient et le reste de la division euclidienne de P par $(X-\alpha)^{m+1}$ ($\deg R_1(X-\alpha)^m < m+1$) et $R_1(X-\alpha)^m \neq 0$ (car le coefficient dominant de $(X-\alpha)^m$ est 1 et $R_1 = \tilde{Q}(\alpha) \neq 0$) alors $(X-\alpha)^m/P$ et $(X-\alpha)^{m+1} \nmid P$.

D'autre part, si K est un corps de caractéristique nulle, $P \in K[X]$ de degré n et α un élément de K, alors α est une racine de P d'ordre de multiplicité égale à m si, et seulement si, $(X-\alpha)^m$ divise P et $(X-\alpha)^{m+1}$ ne divise pas P, i.e., si, et seulement si, $\tilde{P}(\alpha) = ... = \widetilde{P^{(m-1)}}(\alpha) = 0$ et $\widetilde{P^{(m)}}(\alpha) \neq 0$ (cf. théorème 5.20) ∎

Soient A un anneau intègre, P et Q deux éléments de $A[X]$. On rappelle que :

- Q/P si $P = QS$ avec $S \in A[X]$.

- Un polynôme $P \in A[X]$ est irréductible si P est non nul, non inversible et les seuls diviseurs de P sont les éléments inversibles et les associés de P ; i.e., $P \neq 0, P \notin \mathcal{U}(A)$ et si Q/P, alors $Q \in \mathcal{U}(A[X]) = \mathcal{U}(A)$ ou $Q = uP$, avec $u \in \mathcal{U}(A[X]) = \mathcal{U}(A)$.

En particulier, si $A = K$ est un corps (commutatif), Un polynôme $P \in K[X]$ est irréductible si P est non constant et les seuls diviseurs de P sont les constantes non nulles et les associés de P ; i.e., $\deg P \geq 1$ et si Q/P, alors $Q \in \mathcal{U}(K[X]) = K^*$ ou $Q = uP$, avec $u \in K^*$.

Exemple 5.23 *Le polynôme $X^2 - 2$ est irréducible dans $\mathbb{Z}[X]$ (on dit aussi irréductible sur $\mathbb{Z}$) mais $X^2 - 2$ n'est pas irréductible dans $\mathbb{R}[X]$.*

Exercice 5.24

1) Soient A un anneau intègre et $P \in A[X]$ de degré 2. Montrer que si P admet une racine dans A, alors P n'est pas irréductible. Montrer que la réciproque est fausse.

2) Soient K un corps et $P \in K[X]$ de degré 2 ou 3. Montrer que P est irréductible dans $K[X]$ si, et seulement si, P n'a pas de racines dans K.

Proposition et Définition 5.25 *Soit K un corps (commutatif). Les propositions suivantes sont équivalentes :*

(i) Tout polynôme non constant de $K[X]$ possède au moins une racine.

(ii) Tout polynôme non constant de $K[X]$ est scindé dans $K[X]$.

(iii) Les seuls polynômes irréductibles dans $K[X]$ sont les polyômes de degré 1.

Si K vérifie l'une de ces propositions, on dit que K est un ***corps algébriquement clos****.*

Exemple 5.26 *$\mathbb{C}$ est un corps algébriquement clos. Dans $\mathbb{C}[X]$, Les seuls polynômes irréductibles sont les polynômes de degré 1. (**Théorème de d'Alembert-Gauss**).*

Exercice 5.27 *On se propose de montrer que les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degrés 1 et les polynômes $aX^2 + bX + c \in \mathbb{R}[X]$ de degrés 2 tels que $\Delta = b^2 - 4ac < 0$.*

1) Montrer que si $P, Q \in \mathbb{R}[X]$, alors Q divise P dans $\mathbb{R}[X]$ si, et seulement si, Q divise P dans $\mathbb{C}[X]$. (Ind : Utiliser l'unicité du quotient et du reste de la division euclidienne de P par Q dans $\mathbb{C}[X]$).

2) Soit $P = a_0 + a_1X + \ldots + a_nX^n \in \mathbb{R}[X]$.

i) Vérifier que si $\alpha \in \mathbb{C}$, alors $P(\bar{\alpha}) = \overline{P(\alpha)}$ et en déduire que si $\alpha \in \mathbb{C}$ est une racine de P d'ordre de multiplicité égale à m, alors $\bar{\alpha}$ est aussi une racine de P d'ordre de multiplicité égale à m.

ii) En utilisant les questions 1) et 2) i), montrer que les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degrés 1 et les polynômes $aX^2 + bX + c \in \mathbb{R}[X]$ de degrés 2 tels que $\Delta = b^2 - 4ac < 0$.

5.5 Arithmétique dans K[X]

Théorème 5.28 *Si K est un corps (commutatif), alors $K[X]$ est un anneau principal.*

Preuve. Il est évident que $K[X]$ est un anneau intègre. Soit I un idéal de $K[X]$ tel que $I \neq \{0\}$ (si $I = \{0\}$, alors $I = (0)$ est principal). On considère l'ensemble $N = \{\deg P / P \in I - \{0\}\}$. N est une partie non vide de $\mathbb{N}$ et par suite N possède un plus petit élément qu'on note n. Soit $P \in I : \deg P = n$. Montrons que $I = (P)$. Puisque $P \in I, (P) \subset I$. D'autre part, soit S$\in I$, en effectuant la division euclidienne de S par P, on obtient $S = PQ + R$ avec $(Q, R) \in (K[X])^2$ et $\deg R < \deg P = n$. Comme $R = S - PQ \in I$ et $degR < degP = n$, $R = 0$ (n est le plus petit élément de N) ■

Corollaire 5.29 *Soient K un corps (commutatif), P et Q deux polynômes éléments de $K[X]$.*

(i) P et Q admettent un pgcd et un ppcm et,

* *$P \wedge Q = D$ si, et seulement si, $(P) + (Q) = (D)$.*

* *$P \vee Q = M$ si, et seulement si, $(P) \cap (Q) = (M)$.*

*(ii) P et Q sont premiers entre eux si, et seulement si, il existe U et V, deux polynômes éléments de $K[X]$, tels que $UP + VQ = 1$.(**Théorème de Bezout**).*

(iii) Soit S un polynôme élément de $K[X]$.

* *Si $P \wedge Q = 1$ et $P \wedge S = 1$, alors $P \wedge QS = 1$.*

* *Si P/QS et $P \wedge Q = 1$, alors P/S (**Théorème de Gauss**).*

* *Si Q/P et S/P et $Q \wedge S = 1$, alors QS/P.*

(iv)

* *Si P est non constant, alors P s'écrit sous la forme $P = P_1...P_r$, où $P_1, ..., P_r$ sont des polynômes irréductibles, non nécessairement distincts, éléments de $K[X]$.*

* *Si P est non constant et P possède une autre décomposition de type $P = Q_1...Q_s$, où $Q_1, ..., Q_s$ sont des polynômes irréductibles, éléments de $K[X]$, alors $r = s$ et il existe une permutation σ de S_r telle que P_i et $Q_{\sigma(i)}$ sont associés pour tout $i \in \{1, ..., r\}$.*

(v) Les propositions suivantes sont équivalentes :

* *P est irréductible.*

* *P est premier, i.e. Si P/QS, avec $Q, S \in K[X]$, alors P/Q ou P/S.*

* *(P) est un idéal premier de $K[X]$ et $P \neq 0$.*

* *(P) est un idéal maximal de $K[X]$.*

(vi) Si $P = P_1^{\alpha_1}...P_r^{\alpha_1}$, $Q = P_1^{\beta_1}...P_r^{\beta_1} \in K[X]$, avec $P_1, ..., P_r$ des polynômes irréductibles de $K[X]$, $P_i \neq P_j$ si $i \neq j$ et $\alpha_i \geq 0, \beta_i \geq 0$, alors $P \wedge Q = P_1^{\lambda_1}...P_r^{\lambda_1}$, $\lambda_i = \min\{\alpha_i, \beta_i\}$ pour tout $i \in \{1, ..., r\}$ et $P \vee Q = P_1^{\mu_1}...P_r^{\mu_r}$ où $\mu_i = \max\{\alpha_i, \beta_i\}$ pour tout $i \in \{1, ..., r\}$.

Preuve. Comme $K[X]$ est principal, il suffit d'appliquer la proposition 4.15 pour (i), le théorème 4.16 pour (ii), la proposition 4.17 pour (iii), le théorème 4.18 pour (iv), la proposition 4.13, pour (v) et le théorème 4.20 pour (vi) ■

Algorithme d'Euclide

Proposition 5.30 *Soient P et S deux polynômes, non nuls, éléments de K[X] tels que $degS \leq degP$ et S ne divise pas P. Alors $P \wedge S = S \wedge R$, où R est le reste de la division euclidienne de P par S.*

Preuve. Même démonstration que celle de la proposition 1.23 ■

Algorithme 5.31 (Algorithme d'Euclide dans K[X]) *Soient P et S deux polynômes non nuls, éléments de K[X], tels que $degS \leq degP$ et S ne divise pas P. Alors, un pgcd de P et S est le dernier reste non nul obtenu en appliquant l'algorithme d'Euclide. Cet algorithme consiste à :*
** Effectuer la division euclidienne de P par S : $P = SQ_1 + R_1$*
** Effectuer la division euclidienne de S par R_1 : $S = R_1Q_2 + R_2$*
** Effectuer la division euclidienne de R_1 par R_2 : $R_1 = R_2Q_3 + R_3$*
...
La suite (R_i) est telle que $\deg R_{i+1} < \deg R_i$ tant que les R_i sont non nuls. Ainsi il existe $n : R_n \neq 0$ et $R_{n+1} = 0$. D'autre part, on a ,d'après la proposition précédente, $P \wedge S = S \wedge R_1 = \ldots = R_{n-1} \wedge R_n = R_n$.

Exemple 5.32
1) Soient $P = \overline{4}X^3 + \overline{2}X^2 + X + \overline{1}$ et $S = X^3 + \overline{4}X^2$ deux polynômes de $\mathbb{Z}/5\mathbb{Z}[X]$. Utilisons l'algorithme d'Euclide pour déterminer $P \wedge Q$. On a $P = SQ_1 + R_1$ avec $Q_1 = \overline{4}$ et $R_1 = X^2 + X + \overline{1}$, $S = R_1Q_2 + R_2$ avec $Q_2 = X + \overline{3}$ et $R_2 = X + \overline{2}$, $R_1 = R_2Q_3 + R_3$ avec $Q_3 = X + \overline{4}$ et $R_3 = \overline{3}$, $R_2 = R_3.Q_4 + R_4$ avec $Q_4 = \overline{2}X + \overline{4}$ et $R_4 = \overline{0}$. Ainsi, $P \wedge Q = \overline{1}$ ($P \wedge Q = \overline{3}$ et $\overline{3}$ est inversible dans $\mathbb{Z}/5\mathbb{Z}$).
D'autre part, On a $\overline{1} = \overline{2}.\overline{3} = \overline{2}.R_3 = \overline{2}(R_1 - R_2Q_3) = \overline{2}(R_1 - (S - R_1Q_2)Q_3) = \overline{2}(R_1(1 + Q_2Q_3) - SQ_3) = \overline{2}((P - SQ_1)(1 + Q_2Q_3) - SQ_3) = (\overline{2}(1 + Q_2Q_3))P + (\overline{2}(-Q_1 - Q_3 - Q_1Q_2Q_3))S = (\overline{2}X^2 + \overline{4}X + \overline{1})P + (\overline{2}X^2 + \overline{2}X + \overline{3})S$ et ainsi, en posant $U = \overline{2}X^2 + \overline{4}X + \overline{1}$, $V = \overline{2}X^2 + \overline{2}X + \overline{3}$, on a $UP + VS = \overline{1}$.
2) Aussi, comme $\mathbb{Z}/5\mathbb{Z}[X]$ est principal, tout polynôme non constant P, élément de $\mathbb{Z}/5\mathbb{Z}[X]$, se décompose en produit de polynômes irréductibles et deux décompositions de P en produit de polynômes irréductibles ne diffèrent que par l'ordre des facteurs et par des constantes non nuls près. Soit, par exemple, $P = \overline{4}X^3 + \overline{2}X^2 + X + \overline{3} \in \mathbb{Z}/5\mathbb{Z}[X]$, alors $P = (X + \overline{1})(X + \overline{4})(\overline{4}X + \overline{2})$ avec $X + \overline{1}, X + \overline{4}$ et $\overline{4}X + \overline{2}$ sont irréductibles dans $\mathbb{Z}/5\mathbb{Z}[X]$.

5.6 Polynômes irréductibles à coefficients dans un anneau principal

Dans toute cette section, l'anneau A est supposé être principal.

Proposition 5.33 *Soient K le corps des fractions de A et P un polynôme non constant de $A[X]$. Si $P = QS$ avec $Q, S \in K[X]$, alors il existe λ un élément non nul de K tel que λQ et $\lambda^{-1}S$ appartiennent à $A[X]$ et ainsi si P est irréductible dans $A[X]$, alors P est irréductible dans $K[X]$.*

Preuve. Soit $P = QS$ avec $Q, S \in K[X]$. on a $Q = \sum_{i=0}^{r} \frac{a_i}{\alpha_i} X^i$ et $S = \sum_{i=0}^{s} \frac{b_i}{\beta_i} X^i$, où $a_i, b_i \in A, \alpha_i, \beta_i \in A^*$. Posons $a = ppcm(\alpha_0, ..., \alpha_r)$ et $b = ppcm(\beta_0, ..., \beta_s)$, alors $aQ = Q_1 \in A[X]$ $bS = S_1 \in A[X]$ et $abP = Q_1S_1$. Posons $c = ab$ et supposons que c n'est pas inversible (si c est

inversible dans A, a et b sont inversibles dans A et ainsi $Q = a^{-1}Q_1, S = b^{-1}S_1 \in A[X]$), alors $c = p_1 \dots p_t$ avec $p_1, \dots, p_t$ irréductibles dans A. Montrons, par l'absurde, que p_1 divise tous les coefficients de Q_1 ou p_1 divise tous les coefficients de S_1 : Posons $Q_1 = \sum_{j=0}^{r} d_j X^j$ et $S_1 = \sum_{j=0}^{s} e_j X^j$ et supposons que p_1 ne divise pas tous les coefficients de Q_1 et p_1 ne divise pas tous les coefficients de S_1. Soient d_k et e_l les coefficients respectivement de Q_1 et S_1 ayant les plus petits indices et tels que $p_1 \nmid d_k$ et $p_1 \nmid e_l$, alors p_1 ne divise pas le coefficient f_{k+l} de X^{k+l} dans Q_1S_1. En effet, $f_{k+l} = d_0e_{k+l} + d_1e_{k+l-1} + \dots + d_ke_l + \dots + d_{k+l-1}e_1 + d_{k+l}e_0$ et comme p_1 divise tous les termes de cette expression sauf d_ke_l, alors p_1 ne divise pas f_{k+l} ce qui est absurde car c divise tous les coefficients de Q_1S_1. Ainsi p_1 divise tous les coefficients de Q_1 ou p_1 divise tous les coefficients de S_1. Si p_1 divise tous les coefficients de Q_1 (de même pour le cas où p_1 divise tous les coefficients de S_1), alors $\exists Q_1' \in A[X] : Q_1 = p_1Q_1'$, $p_1 \dots p_tP = p_1Q_1'S_1$ et $p_2 \dots p_tP = Q_1'S_1$. En reprenant le même raisonement pour p_2, ..., et p_t, on obtient, $P = Q_2S_2$ avec $Q_2, S_2 \in A[X]$. Vu que pour passer de Q à Q_2, on n'a utilisé que la division par des éléments non nuls de A alors $\exists \lambda \in K : Q_2 = \lambda Q$ et aussi $S_2 = \lambda^{-1}S$.

Soient P un polynôme non constant et irréductible dans $A[X]$ et $Q \in K[X]$ tels que Q/P, alors $\exists S \in K[X] : P = QS$ d'où il existe $\lambda \in K^*$ tel que $\lambda Q, \lambda^{-1}S \in A[X]$ et $P = (\lambda Q)(\lambda^{-1}S)$, alors $\lambda Q = u \in \mathcal{U}(A)$ ou $\lambda Q = uP$ avec $u \in \mathcal{U}(A)$ (car P est irréductible dans $A[X]$) et ainsi $Q = u\lambda^{-1} \in K^*$ ou $Q = vP$ avec $v \in K^*$ $(v = u\lambda^{-1})$ ■

Définition 5.34 *Soit $P = a_0 + a_1X + ... + a_nX^n$ un polynôme non constant de $A[X]$. On appelle **contenu de** P et on note* $\mathbf{c(P)}$ *un pgcd des coefficients de P ; i.e., $c(P) = pgcd(a_0, ..., a_n)$.*

*On dit que le polynôme P est **primitif** dans $A[X]$ si $c(P) = 1$.*

Exemple 5.35 *Le polynôme $3X^2 + 4X + 12 \in \mathbb{Z}[X]$ est primitif mais $4X + 12$ ne l'est pas.*

Remarque 5.36 *Soit $P = a_0 + a_1X + ... + a_nX^n$ un polynôme non constant de $A[X]$. Si P n'est pas primitif dans $A[X]$, alors P n'est pas irréductible. En effet, $c(P)/P$ et $c(P)$ n'est ni inversible (car P n'est pas primitif) ni associé à P (car $\deg(c(P)) = 0$ et $\deg P \geq 1$).*

Exercice 5.37 *Soient A un anneau principal et $P \in A[X]$ primitif non constant. Montrer que si $a \in A$ divise P, alors $a \in \mathcal{U}(A)$.*

Les deux résultats suivants donnent deux critères d'irréductibilité des polynômes à coefficients dans un anneau principal.

Soient A un anneau principal, p un élément de A et φ l'application de $A[X]$ vers $(A/(p))[X]$ définie par $\varphi(\sum_{i=0}^{n} a_iX^i) = \sum_{i=0}^{n} \overline{a_i}X^i$, où $\overline{a_i}$ est la classe de a_i modulo l'idéal (p). ($\varphi(P)$ est appelée **la réduction modulo p** du polynôme P). Il est évident que φ est un homomorphisme d'anneaux.

Soit $P = \sum_{i=0}^{n} a_iX^i \in A[X]$ de degré n, alors $deg(\varphi(P)) = \sum_{i=0}^{n} \overline{a_i}X^i \leq n$ et on a $\deg(\varphi(P)) = \deg(P)$ si, et seulement si, $\overline{a_n} \neq \bar{0}$, i.e. $p \nmid a_n$.

Proposition 5.38 (Réduction modulo p) *Soient p un élément premier de A, φ l'homomorphisme d'anneaux de $A[X]$ vers $(A/(p))[X]$ défini par $\varphi(\sum_{i=0}^{n} a_iX^i) = \sum_{i=0}^{n} \overline{a_i}X^i$, où $\overline{a_i}$ est la classe de a_i modulo l'idéal (p) et $P = \sum_{i=0}^{n} a_iX^i \in A[X]$ un polynôme primitif de degré $n \geq 1$ tel que $p \nmid a_n$.*

Si $\varphi(P)$ est irréductible dans $(A/(p))[X]$, alors P est irréductible dans $A[X]$.

Preuve. Puisque $\deg P \geq 1$, P est non nul et non inversible. Soit $Q \in A[X] : Q/P$, alors $\exists S \in A[X]$: $P = QS$. Posons $Q = \sum_{i=0}^{m} b_i X^i$ avec $b_m \neq 0$ et $S = \sum_{i=0}^{l} c_i X^i$ avec $c_l \neq 0$. Puisque $p \nmid a_n$, $p \nmid b_m$ et $p \nmid c_l$ $(a_n = b_m c_l)$, ainsi $\deg \varphi(Q) = \deg Q$ et $\deg \varphi(S) = \deg S$.

Comme $\varphi(P) = \varphi(QS) = \varphi(Q)\varphi(S)$ et $A/(p)$ est intègre (p est premier), alors $\varphi(Q) \in \mathcal{U}((A/(p)[X]) = \mathcal{U}(A/(p))$ ou $\varphi(S) \in \mathcal{U}((A/(p)[X]) = \mathcal{U}(A/(p))$ ($\varphi(P)$ est irréductible dans $(A/(p))[X]$) et par suite $Q = b_m \in A$ ou $S = c_l \in A$ (car $\deg \varphi(Q) = \deg Q$ et $\deg \varphi(S) = \deg S$). Comme P est primitif, $Q \in \mathcal{U}(A)$ ou $S \in \mathcal{U}(A)$ (cf. exercice 5.37) et ainsi P est irréductible dans $A[X]$ ■

Exemple 5.39 *Le polynôme $P = X^3 + X + 15$ est irréductible dans $\mathbb{Q}[X]$. En effet, $P = X^3 + X + 15 \in \mathbb{Z}[X]$ ($\mathbb{Z}$ est principal) et P est primitif. On prend $p = 2$ un nombre premier et on note $\varphi(P)$ la réduction modulo 2 de P. On a $\varphi(P) = X^3 + X + \bar{1} \in (\mathbb{Z}/2\mathbb{Z})[X]$. Puisque $\mathbb{Z}/2\mathbb{Z}$ est un corps, $\deg \varphi(P) = 3$ et $\varphi(P) = X^3 + X + \bar{1}$ n'a pas de racines dans $(\mathbb{Z}/2\mathbb{Z})$, $\varphi(P)$ est irréductible dans $(\mathbb{Z}/2\mathbb{Z})[X]$ et par suite $P = X^3 + X + 15$ est irréductible dans $\mathbb{Z}[X]$ et ainsi $P = X^3 + X + 15$ est irréductible dans $\mathbb{Q}[X]$ car $\mathbb{Q} = Fr(\mathbb{Z})$ (cf. proposition 5.33).*

Remarque 5.40

1) L'exemple suivant montre que la condition $p \nmid a_n$ est importante : soit $P = 2X^2 + X - 1 \in \mathbb{Z}[X]$. En posant $p = 2$, on a $\varphi(P) = X + \bar{1} \in \mathbb{Z}/2\mathbb{Z}[X]$ est irréductible dans $\mathbb{Z}/2\mathbb{Z}[X]$. Cependant, $P = 2X^2 + X - 1$ n'est pas irréductible dans $\mathbb{Z}[X]$ $(X + 1/2X^2 + X - 1)$.

2) La réciproque de la proposition précédente est fausse. En effet, soit $P = X^2 + 2 \in \mathbb{Z}[X]$. En posant $p = 2$, $\varphi(P) = X^2 \in \mathbb{Z}/2\mathbb{Z}[X]$, $p = 2 \nmid 1 = a_n$ et on a P est irréductible dans $\mathbb{Z}[X]$ mais, $\varphi(P) = X^2$ n'est pas irréductible dans $\mathbb{Z}/2\mathbb{Z}[X]$.

Proposition 5.41 (Critère d'Eisenstein) *Soient A un anneau principal, K son corps des fractions et $P = a_0 + a_1 X + ... + a_n X^n$ un polynôme non constant et primitif de $A[X]$.*

On suppose qu'il existe p un élément premier de A tel que :

(i) p/a_i $\forall i = 0, 1, ..., n-1$,

(ii) $p \nmid a_n$ et

(iii) $p^2 \nmid a_0$.

Alors P est irréducible dans $A[X]$.

Preuve. Puisque $\deg P \geq 1$, P est non nul et non inversible. Soit $Q \in A[X] : Q/P$ alors $\exists S \in A[X]$: $P = QS$. Posons $Q = \sum_{i=0}^{m} b_i X^i$ avec $b_m \neq 0$ et $S = \sum_{i=0}^{l} c_i X^i$ avec $c_l \neq 0$.

Supposons que $\deg Q \geq 1$ et $\deg S \geq 1$. Comme $p/a_0 = b_0 c_0$, p/b_0 ou p/c_0 (p est premier) et puisque $p \nmid a_n$, $p \nmid b_m$ et $p \nmid c_l$ $(a_n = b_m c_l)$.

On suppose que p/b_0 (de même si p/c_0). Soient $N = \{i \in \{0, ..., m\} / \ p \nmid b_i\}$ et $r = \inf N$ ($N \neq \emptyset$ car $m \in N$). On a $r \leq m < n$ ($m < n$ car $n = m + l$ et $l \geq 1$) d'où p/a_r.

D'autre part, $a_r = b_r c_0 + \sum_{\substack{i+j=r \\ i<r}} b_i c_j$ et comme p/a_r et p/b_i, $\forall i < r$, $p/a_r - \sum_{\substack{i+j=r \\ i<r}} b_i c_j = b_r c_0$ d'où p/b_r ou p/c_0 car p est premier. Or $p \nmid b_r$ ($r \in N$) et $p \nmid c_0$ (sinon $p^2/b_0 c_0 = a_0$). Ainsi, $Q \in A$ ou $S \in A$ et puisque P est primitif $Q \in \mathcal{U}(A)$ ou $S \in \mathcal{U}(A)$ ■

Exemple 5.42 *Soient p un nombre premier et $n \in \mathbb{N}^*$. Alors $P(X) = X^n - p \in \mathbb{Q}[X]$ est irréductible dans $\mathbb{Q}[X]$. En effet, $P(X) = X^n - p \in \mathbb{Z}[X]$ est primitif et on a : $p / -p$, $p \nmid 1$ et $p^2 \nmid p$, alors $P(X) = X^n - p$ est irréductible dans $\mathbb{Z}[X]$ et par suite $P(X) = X^n - p$ est irréductible dans $\mathbb{Q}[X]$.*

Exercice 5.43 *Soient A un anneau principal et P, Q deux polynômes non constants de $A[X]$.*

1) Montrer que si $P = \alpha P_1$, où α est un élément de A et P_1 un polynôme primitif de $A[X]$, alors α est un contenu de P. (Ind : Utiliser $pgcd(\alpha a, \alpha b) = \alpha\ pgcd(a, b)$).

2) Montrer que

(i) Si P et Q sont primitifs, alors PQ est primitif. (Ind : Utiliser un raisonnement par l'absurde et considérer l'homomorphisme $\varphi : A[X] \longrightarrow (A/(p))[X]$ défini par $\varphi(\sum_{i=0}^{n} a_i X^i) = \sum_{i=0}^{n} \overline{a_i} X^i$, où $\overline{a_i}$ est la classe de a_i modulo l'idéal (p) avec p un élément premier tel que $p/c(PQ)$).

*(ii) $c(PQ) = c(P)c(Q)$. (**lemme de Gauss**). (Ind : Utiliser 2)i) et 1)).*

3) Soit K le corps des fractions de A. Montrer que P est irréductible dans $A[X]$ si, et seulement si, P est primitif dans $A[X]$ et P est irréductible dans $K[X]$. (Ind : Utiliser le lemme de Gauss).

4) En déduire que les polynômes irréductibles de $A[X]$ sont :

- Les éléments p de A irréductibles dans A,

- Les polynômes non constants de $A[X]$, primitifs dans $A[X]$ et irréductibles dans $K[X]$.

Remarque 5.44 *Dans tous les résultats et toutes les définitions de cette section (et aussi dans l'exercice précédent), on n'utilise que le fait que A est intègre et que A vérifie les conditions (i) et (ii) de la proposition 4.18, i.e. A est factoriel. Ainsi, on peut remplacer, dans ce qui précéde, la condition "A est principal" par "A est factoriel" et obtenir tous ces résultats.*

Chapitre 6

Anneau de polynômes à deux ou trois indéterminées

A désigne un anneau commutatif (unitaire et non trivial).

6.1 Construction et Définitions

6.1.1 Construction

Soient $B = A[X]$ l'anneau de polynômes à une indéterminée X à coefficients dans A et P un polynôme élément de l'anneau $B[Y] = (A[X])[Y]$ de polynômes à une indéterminée Y à coefficients dans $B = A[X]$. Alors $P = \sum_{j=0}^{m} b_j Y^j$ avec $b_j \in B = A[X]$. On pose $b_j = \sum_{i=0}^{n} a_{ij} X^i$ avec $a_{ij} \in A$, ainsi $P = \sum_{i=0}^{n}\sum_{j=0}^{m} a_{ij} X^i Y^j$ avec $a_{ij} \in A$ et on a, $P = 0$ si, et seulement si, $b_j = 0$ $\forall j \in \{0, \ldots, m\}$ si, et seulement si, $a_{ij} = 0$ $\forall i \in \{0, \ldots, n\}$, $\forall j \in \{0, \ldots, m\}$.

L'anneau $B[Y] = (A[X])[Y]$, noté $A[X, Y]$, est appelé **anneau de polynômes à deux indéterminées X et Y, à coefficients dans l'anneau A**. Un polynôme de $A[X, Y]$ de la forme $a_{ij} X^i Y^j$ est appelé **monôme** de $A[X, Y]$. Si $a_{ij} = 1$, on dit que $X^i Y^j$ est un monôme unitaire.

D'une manière analogue à celle décrite ci-dessus, on construit l'anneau $A[X, Y, Z] = (A[X, Y])[Z]$ appelé **anneau de polynômes à trois indéterminées X, Y et Z, à coefficients dans l'anneau A**. Aussi, si P est un polynôme élément de $A[X, Y, Z]$ alors $P = \sum_{i=0}^{n}\sum_{j=0}^{m}\sum_{k=0}^{l} a_{ijk} X^i Y^j Z^k$ avec $a_{ijk} \in A$ et $P = 0$ si, et seulement si, $a_{ijk} = 0$ $\forall i \in \{0, \ldots, n\}$, $\forall j \in \{0, \ldots, m\}$, $\forall k \in \{0, \ldots, l\}$.

Un polynôme de $A[X, Y, Z]$ de la forme $a_{ijk} X^i Y^j Z^k$ de $A[X, Y, Z]$ est appelé **monôme** et $X^i Y^j Z^k$ est appelé monôme unitaire.

Exemple 6.1 *$P = X + 3Y + XY^3 \in \mathbb{Z}[X, Y]$ est un polynôme à deux indéterminées à coefficients dans $\mathbb{Z}$ et $Q = Y + \overline{2}YZ + \overline{3}X^2Z^3 \in (\mathbb{Z}/4\mathbb{Z})[X, Y, Z]$ est un polynome à trois indéterminées à coefficients dans $\mathbb{Z}/4\mathbb{Z}$. Les polynômes $Y, \overline{2}YZ$ et $\overline{3}X^2Z^3$ sont les monômes de Q.*

Remarque 6.2

1) L'anneau $A[X]$ est un sous-anneau de l'anneau $(A[X])[Y] = A[X, Y]$ et $A[X, Y]$ est un sous-anneau de $(A[X, Y])[Z] = A[X, Y, Z]$.

2) Puisque $A[X,Y] = (A[X])[Y]$ (resp. $A[X,Y,Z] = (A[X,Y])[Z]$), si A est intègre alors $A[X,Y]$ (resp. $A[X,Y,Z]$) est un anneau intègre. En particulier, si $A = K$ est un corps (commutatif), $K[X,Y]$ (resp. $K[X,Y,Z]$) est intègre.

3) Pour $n \geq 4$, on définit par récurrence l'anneau $A[X_1, \ldots, X_n]$ de polynômes à n indéterminées $X_1, \ldots$ et X_n, à coefficients dans l'anneau A comme étant l'anneau de polynômes à une indéterminée X_n à coefficients dans $A[X_1, \ldots, X_{n-1}]$.

6.1.2 Degré partiel et Degré total

Définitions 6.3

*- Soit $Q = a_{ij}X^iY^j \in A[X,Y]$ (resp. $Q = a_{ijk}X^iY^jZ^k \in A[X,Y,Z]$) un monôme non nul de $A[X,Y]$ (resp. un monôme non nul de $A[X,Y,Z]$). Les entier i et j (et k si $Q = a_{ijk}X^iY^jZ^k \in A[X,Y,Z]$) sont appelés respectivement **degré partiel** du monôme Q en X ou simplement degré de Q par rapport à X, **degré partiel** de Q en Y (et degré partiel de Q en Z si $Q = a_{ijk}X^iY^jZ^k \in A[X,Y,Z]$).*

*L'entier $i+j$ (resp. l'entier $i+j+k$) est appelé **degré total** du monôme Q ou simplement degré du monôme Q.*

*- Soit $P \in A[X,Y]$ un polynôme non nul de $A[X,Y]$ (resp. $P \in A[X,Y,Z]$). On appelle **degré partiel** de P en X et on le note $\deg_X P$, le sup des degré partiaux des monômes non nuls du polynôme P. De la même façon, on définit le degré partiel de P en Y, le degré partiel de P en Z et on les note respectivement $\deg_Y P$ et $\deg_Z P$.*

*On appelle **degré total** du polynôme P ou simplement **degré** du polynôme P, et on le note $\deg P$, le sup des degrés des monômes non nuls de P. Si P est nul, on pose $\deg P = -\infty$.*

Exemple 6.4

1) Si $P \in A$ et P est non nul, $\deg_X P = \deg_Y P = \deg_Z P = \deg P = 0$.

2) Soit $P = X + 3Y^4 + XY^3 \in \mathbb{Z}[X,Y]$, alors $\deg_X P = 1$, $\deg_Y P = 4$ et $\deg P = 4$.

3) Soit $Q = Y + \overline{2}YZ + \overline{3}X^2Z^3 \in \mathbb{Z}/4\mathbb{Z}[X,Y]$ alors $\deg_X Q = 2$, $\deg_Y Q = 1$, $\deg_Z Q = 3$ et $\deg Q = 5$.

Définition 6.5 *Un polynôme non nul P élément de $A[X,Y]$ (resp. de $A[X,Y,Z]$) est dit **homogène** de degré n si tous les monômes de P ont un même degré égal à n.*

Proposition 6.6

(i) Si $P \in A[X,Y]$ (resp. $P \in A[X,Y,Z]$) est un polynôme non nul de degré n alors P s'écrit de façon unique sous la forme : $P = P_0 + P_1 + \ldots + P_n$, où $P_i \in A[X,Y]$ (resp. $P_i \in A[X,Y,Z]$), P_n homogène de degré n et $\forall i = 0, ..., n-1 : P_i = 0$ ou P_i est homogène de degré i.

(ii) Si $P, Q \in A[X,Y]$ (resp. $P, Q \in A[X,Y,Z]$) sont deux polynômes homogènes de degrés respectivement n et m, alors $PQ = 0$ ou PQ est un polynôme homogène de degré $n+m$.

Preuve. (i) Soit $P = \sum_{i+j+k=0}^{n} a_{ijk}X^iY^jZ^k \in A[X,Y,Z]$, alors $P = a_{000} + (a_{100}X + a_{010}Y + a_{001}Z) + ... + (\sum_{i+j+k=l} a_{ijk}X^iY^jZ^k) + ... + (\sum_{i+j+k=n} a_{ijk}X^iY^jZ^k)$. Posons $P_0 = a_{000}$, $P_1 = (a_{100}X + a_{010}Y + a_{001}Z), ..., P_l = \sum_{i+j+k=l} a_{ijk}X^iY^jZ^k, ...$ et $P_n = \sum_{i+j+k=n} a_{ijk}X^iY^jZ^k$, alors $P = P_0 + P + \ldots + P_n$, avec $\forall i = 0, ..., n-1 : P_i = 0$ ou P_i est homogène de degré i. Puisque P est de degré n, alors $P_n \neq 0$ et P_n est homogène de degré n.

Si $P = P_0 + P_1 + \ldots + P_n = Q_0 + Q_1 + \ldots + Q_n$, $0 = (P_0 - Q_0) + (P_1 - Q_1) + \ldots + (P_n - Q_n)$ et alors $\forall i = 0, ..., n : P_i - Q_i = 0$. En effet, supposons qu'il existe $i : P_i - Q_i \neq 0$, alors $P_i - Q_i$ est

homogène de degré i. Puisque $\deg(P_i - Q_i) = i \neq \deg(P_j - Q_j)$ $\forall j \neq i$, $(P_0 - Q_0) + (P_1 - Q_1) + \ldots + (P_{i-1} - Q_{i-1}) + (P_i - Q_i) + (P_{i+1} - Q_{i+1}) + \ldots + (P_n - Q_n) \neq 0$.

(ii) Faisons la démonstration pour $P, Q \in A[X,Y,Z]$. Posons $P = \sum_{i_1+j_1+k_1=n} a_{i_1j_1k_1} X^{i_1} Y^{j_1} Z^{k_1}$, $Q = \sum_{i_2+j_2+k_2=m} b_{i_2j_2k_2} X^{i_2} Y^{j_2} Z^{k_2} \in A[X,Y,Z]$ de degrés respectivement n et m. Alors

$$PQ = \sum_{\substack{i_1+j_1+k_1=n\\ i_2+j_2+k_2=m}} a_{i_1j_1k_1} b_{i_2j_2k_2} X^{i_1+i_2} Y^{j_1+j_2} Z^{k_1+k_2} = \sum_{l+s+t=n+m} \Big(\sum_{\substack{i_1+i_2=l\\ j_1+j_2=s\\ k_1+k_2=t}} a_{i_1j_1k_1} b_{i_2j_2k_2} \Big) X^l Y^s Z^t \text{ et}$$

ainsi si $PQ \neq 0$, PQ est un polynôme homogène de degré $n + m$ ■

Proposition 6.7 *Si P et Q sont des polynômes de $A[X,Y]$ (resp. de $A[X,Y,Z]$) alors,*

(i) $\deg_X(P + Q) \leq \sup(\deg_X P, \deg_X Q)$ *(de même pour le degré partiel en Y et en Z).*

(ii) $\deg_X(P.Q) \leq \deg_X P + \deg_X Q$ *(de même pour le degré partiel en Y et en Z).*

(iii) $\mathcal{U}(A) \subset A[X] \subset \mathcal{U}(A[X,Y]) \subset \mathcal{U}(A[X,Y,Z])$.

(iv) $\deg(P + Q) \leq \sup(\deg P, \deg Q)$.

(v) $\deg(P.Q) \leq \deg P + \deg Q$.

(vi) si A est intègre alors,

* $\deg_X(P.Q) = \deg_X P + \deg_X Q$, *$\forall P, Q \in A[X,Y]$ (resp. $\forall P, Q \in A[X,Y,Z]$).*

* $\deg(P.Q) = \deg P + \deg Q$, *$\forall P, Q \in A[X,Y]$ (resp. $\forall P, Q \in A[X,Y,Z]$).*

* $\mathcal{U}(A[X,Y,Z]) = \mathcal{U}(A[X,Y]) = \mathcal{U}(A)$ *(en particulier si $A = K$ est un corps alors $\mathcal{U}(K[X,Y,Z]) = \mathcal{U}(K[X,Y]) = K^*$).*

Preuve. Puisque $A[X,Y] = (A[X])[Y]$ et $A[X,Y,Z] = (A[X,Y])[Z]$, les propriétés (i), (ii) et (ii) découlent immédiatement de la proposition 5.5 et la remarque 6.2.

Pour le reste, montrons par exemple le résultat (v). Supposons que $P \neq 0$ et $Q \neq 0$ (le cas où $P = 0$ ou $Q = 0$ est trivial), alors $P = P_0 + P_1 + \ldots + P_n$ avec P_n homogène de degré $n = \deg P$ et $\forall i = 0, ..., n-1$: $P_i = 0$ ou P_i est homogène de degré i, $Q = Q_0 + Q_1 + \ldots + Q_m$ avec Q_m homogène de degré $m = \deg Q$ et $\forall i = 0, ..., m-1$: $Q_i = 0$ ou Q_i est homogène de degré i. Ainsi $PQ = P_0Q_0 + (P_0Q_1 + P_1Q_0) + ... + \sum_{i+j=l} P_iQ_j + ... + (P_{n-1}Q_m + P_nQ_{m-1}) + P_nQ_m$ avec $\sum_{i+j=k} P_iQ_j$ est nul ou homogène de degré k. Par conséquent, $\deg(PQ) \leq n + m$ ■

Exercice 6.8 *Montrer que si A est intègre, alors tout diviseur d'un polynôme homogène P dans l'anneau $A[X,Y]$ (resp. dans $A[X,Y,Z]$) est un polynôme homogène. (Ind : Soit Q un diviseur de P, alors $P = QS$. Ecrire $Q = Q_q + Q_{q+1} + \ldots + Q_m$, $S = S_s + S_{s+1} + \ldots + S_t$ avec $q \leq m, s \leq t, Q_q \neq 0$, $Q_m \neq 0, S_s \neq 0, S_t \neq 0, Q_i$ (resp. S_i) nul ou homogène de degré i, et en supposant que Q n'est pas homogène, i.e. $q < m$, remarquer que $\deg(Q_qS_s) < \deg(Q_mS_t)$ et conclure).*

6.2 Fonction polynôme

Soient $(\mathcal{A}(A \times A, A), +, .)$ (resp. $(\mathcal{A}(A \times A \times A, A), +, .)$) l'anneau des applications de A^2 dans A (resp. l'anneau des applications de A^3 dans A) et $P(X,Y) = \sum_{i+j=0}^{n} a_{ij} X^i Y^j \in A[X,Y]$ (resp. $P(X,Y,Z) = \sum_{i+j+k=0}^{n} a_{ijk} X^i Y^j Z^k \in A[X,Y,Z]$). On considère l'application notée $\tilde{P} : A^2 \longrightarrow A, (\alpha, \beta) \longmapsto \tilde{P}(\alpha, \beta) = \sum_{i+j=0}^{n} a_{ij} \alpha^i \beta^j$ (resp. $\tilde{P} : A^3 \longrightarrow A, (\alpha, \beta, \gamma) \longmapsto \tilde{P}(\alpha, \beta, \gamma) =$

$\sum_{i+j+k=0}^{n} a_{ijk}\alpha^i\beta^j\gamma^k$). L'application $\tilde{P}$ est appelée **fonction polynôme associée au polynôme P**.
L'élément $\tilde{P}(\alpha,\beta) = \sum_{i+j=0}^{n} a_{ij}\alpha^i\beta^j$ (resp. $\tilde{P}(\alpha,\beta,\gamma) = \sum_{i+j+k=0}^{n} a_{ijk}\alpha^i\beta^j\gamma^k$) obtenu par **substitution** de α en X et de β en Y (resp. par substitution de α en X, de β en Y et de γ en Z) est appelé valeur de $\tilde{P}$ en (α,β) (resp. valeur de $\tilde{P}$ en (α,β,γ)).

Remarque 6.9 *On a $1 \notin (X,Y)$, où (X,Y) est l'idéal de $K[X,Y]$ (resp. L'idéal de $K[X,Y,Z]$) engendré par X et Y. En effet, supposons qu'il existe $P,Q \in K[X,Y]$ (resp. $P,Q \in K[X,Y,Z]$) tels que $XP+YQ = 1$ alors, $1 = 0.\widetilde{P}(0,0) + 0.\widetilde{Q}(0,0) = 0$ (resp. $1 = 0.\widetilde{P}(0,0,0) + 0.\widetilde{Q}(0,0,0) = 0$), ce qui est faux. De même, on vérifie aussi que $1 \notin (X,Y,Z)$, où (X,Y,Z) est l'idéal de $K[X,Y,Z]$) engendré par X, Y et Z.*

Exercice 6.10 *Vérifier que si $P(X,Y,Z) \in A[X,Y,Z]$ est homogène, alors $Q(X,Y) = P(X,Y,0) \in A[X,Y]$ est nul ou homogène.*

6.3 Factorisation

Soit A un anneau intègre. On rappelle (cf. chapitre 4, définition 4.4) qu'un polynôme $P \in A[X,Y]$ (resp. $P \in A[X,Y,Z]$) est dit irréductible si $P \neq 0, P \notin \mathcal{U}(A[X,Y]) = \mathcal{U}(A)$ (resp. $P \notin \mathcal{U}(A[X,Y,Z]) = \mathcal{U}(A)$) et si $\forall Q \in A[X,Y]$ (resp. $\forall Q \in A[X,Y,Z]$) tel que Q/P, alors $Q \in \mathcal{U}(A[X,Y]) = \mathcal{U}(A)$ (resp. $Q \in \mathcal{U}(A[X,Y,Z]) = \mathcal{U}(A)$) ou $Q = uP$ avec $u \in \mathcal{U}(A[X,Y]) = \mathcal{U}(A)$ (resp. $u \in \mathcal{U}(A[X,Y,Z]) = \mathcal{U}(A)$).

En particulier, si $A = K$ est un corps, alors un polynôme $P \in K[X,Y]$ (resp. $P \in K[X,Y,Z]$) est irréductible si $P \notin K$, et si $\forall Q \in K[X,Y]$ (resp. $\forall Q \in K[X,Y,Z]$) tel que Q/P alors $Q \in K^*$ ou $Q = uP$ avec $u \in K^*$.

Exemple 6.11

1) Soit A un anneau intègre. Si $P \in A[X]$ est un polynôme irréductible dans $A[X]$, alors P est irréductible dans $A[X,Y] = (A[X])[Y]$ et est aussi irréductible dans $A[X,Y,Z] = (A[X,Y])[Z]$. Ainsi, par exemple, X et Y sont irréductibles dans $A[X,Y]$ et dans $A[X,Y,Z]$ et Z est irréductible dans $A[X,Y,Z]$.

2) Soient A un anneau intègre. Alors X et Y sont premiers entre eux dans $A[X,Y]$ (resp. dans $A[X,Y,Z]$). En effet, soit $D \in A[X,Y] : D/X$ et D/Y, alors $\exists P,Q \in A[X,Y] : X = PD$ et $Y = QD$ et en passant aux degrés, on a $1 = \deg P + \deg D$ d'où $\deg D \in \{0,1\}$. On remarque aussi que $\deg D \neq 1$, sinon $\deg P = 0$, i.e., $P = a \in A - \{0\}$ et puisque $X = aD$, $a \in \mathcal{U}(A)$ et ainsi $D = a^{-1}X$. Mais $a^{-1}X \nmid Y$. Donc $\deg D = 0$, i.e., $D = a \in A - \{0\}$ et puisque $X = Pa$, $D = a/1$. De la même façon, on vérifie que X et Z (et aussi Y et Z) sont premiers entre eux dans $A[X,Y,Z]$.

3) Soient K un corps. Si $P \in K[X,Y]$ (resp. $P \in K[X,Y,Z]$) est un polynôme de degré 1, alors P est irréductible dans $K[X,Y]$ (resp. P est irréductible dans $K[X,Y,Z]$).

En effet, $P \notin K$ car $\deg P = 1$. Si $Q \in K[X,Y]$ (resp. $Q \in K[X,Y,Z]$) est tel que Q/P alors il existe S élément de $K[X,Y]$ (resp. $S \in K[X,Y,Z]$) tel que $P = QS$. Puisque $K[X,Y]$ (resp. $K[X,Y,Z]$) est intègre, $1 = \deg Q + \deg S$. D'où $\deg Q = 0$ ou $\deg S = 0$, i.e. $Q = c \in K^*$ ou $S = c \in K^*$.

4) Soit $P(X,Y) = X^2 + Y^2 + 1 \in \mathbb{C}[X,Y]$. Posons $A = \mathbb{C}[X]$ et $p = X - i \in A$, alors p est irréductible dans A car $p = X - i$ est de degré 1. En écrivant $P(X,Y) = Y^2 + (X^2+1)$, on voit que $p/(X^2+1), p \nmid 1$ et $p^2 = (X-i)^2 \nmid (X^2+1)$. Comme $A = \mathbb{C}[X]$ est principal et $P(X,Y) = Y^2 + (X^2+1) \in A[Y]$ est primitif alors, en appliquant le critère d'Eisenstein, $P(X,Y)$ est irréductible dans $A[Y] = \mathbb{C}[X,Y]$.

5) Soit $P(X,Y,Z) = X^3(Y-Z)+Y^3(Z-X)+Z^3(X-Y) \in \mathbb{C}[X,Y,Z]$. *Décomposons* $X^3(Y-Z)+Y^3(Z-X)+Z^3(X-Y)$ *en un produit de polynômes irréductibles dans* $\mathbb{C}[X,Y,Z]$.

Afin de simplifier les calculs, remarquons que $P(X,Y,Z)$ *est un polynôme homogène de degré* 4. *Ainsi, si* $Q \in \mathbb{C}[X,Y,Z]$ *est tel que* Q/P *alors* Q *est homogène (cf. exercice 6.9). Soit* Q/P *tel que* $\deg Q = 1$, $\exists S \in \mathbb{C}[X,Y,Z] : P = QS$. *Alors* Q *est homogène de degré 1 et* S *est homogène de degré 3.*

Posons $Q = aX+bY+cZ$ *et* $S = a'X^3+b'Y^3+c'Z^3+dX^2Y+d'XY^2+f'X^2Z+g'XZ^2+h'Y^2Z+k'YZ^2+l'XYZ$ *; comme* $QS = P$, *on peut prendre* $a=b=c=1$ *et* $a'=b'=c'=l'=0, g'=h'=d=1, d'=f'=k'=-1$ *et donc* $Q = X+Y+Z$ *et* $S = X^2Y-XY^2-X^2Z+XZ^2+Y^2Z-YZ^2$.

En utilisant la même méthode pour le pôlynome S, *on obtient* $S = (X-Y)(XY-XZ-YZ+Z^2)$.

Aussi, on obtient $XY-XZ-YZ+Z^2 = (X-Z)(Y-Z)$ *ce qui donne la décomposition* $P = (X+Y+Z)(X-Y)(X-Z)(Y-Z)$ *avec* $(X+Y+Z),(X-Y),(X-Z),(Y-Z)$ *irréductibles dans* $\mathbb{C}[X,Y,Z]$.

Remarque 6.12 *On rappelle que si* K *est un corps, alors* $K[X]$ *est un anneau principal. Cependant, l'anneau* $K[X,Y]$ *(resp.* $K[X,Y,Z]$*) n'est pas principal car, par exemple, l'idéal* $I = (X,Y)$ *de* $K[X,Y]$ *(resp. de* $K[X,Y,Z]$*) n'est pas principal. En effet, si* I *est principal il existe* $P \in K[X,Y]$ *(resp.* $P \in K[X,Y,Z]$*) tel que* $I = (X,Y) = (P)$. *D'où* P/X *et* P/Y *et alors* $P = c \in K^*$ *et ainsi* $I = (X,Y) = (P) = K[X,Y]$, *ce qui est absurde car* $1 \notin (X,Y)$.

Aussi, on peut prouver que $K[X,Y]$ *(resp.* $K[X,Y,Z]$*) n'est pas principal en remarquant que* $K[X,Y]$ *(resp.* $K[X,Y,Z]$*) ne vérifie pas l'égalité de Bezout. En effet,* X *et* Y *sont premiers entre eux (cf. exemple 2) ci-dessus) mais* $\forall P,Q \in K[X,Y]$ *(resp.* $\forall P,Q \in K[X,Y,Z]$*),* $XP+YQ \neq 1$.

6.4 Polynômes Symétriques

Définition 6.13

- Soit P *un polynôme élément de* $A[X,Y]$. *On dit que* P *est un* ***polynôme symétrique*** *si* $P(X,Y) = P(Y,X)$.

- Soit P *un polynôme élément de* $A[X,Y,Z]$. *On dit que* P *est un* ***polynôme symétrique*** *si* $P(X,Y,Z) = P(Y,X,Z) = P(Z,Y,X)$.

Exemple 6.14 *1) Le polynômes* $5X+5Y+3XY \in \mathbb{Z}[X,Y]$ *est un polynôme symétrique.*

2) Le polynôme $X+2Y+Z \in \mathbb{Z}[X,Y,Z]$ *n'est pas un polynôme symétrique.*

3) Les polynômes $\sigma_1 = X+Y$ *et* $\sigma_2 = XY$ *éléments de* $A[X,Y]$ *sont des polynômes symétriques appelés* ***polynômes symétriques élémentaires*** *de* $A[X,Y]$.

4) Soit $A[X,Y,Z]$ *l'anneau de polynômes à trois indéterminées à coefficients dans l'anneau* A. *Les polynômes* $\sigma_1 = X+Y+Z$, $\sigma_2 = XY+YZ+XZ$ *et* $\sigma_3 = XYZ$ *éléments de* $A[X,Y,Z]$ *sont des polynômes symétriques appelés* ***polynômes symétriques élémentaires*** *de* $A[X,Y,Z]$.

Remarque 6.15

1) Dans le cas général, on dit qu'un polynôme $P \in A[X_1,\ldots,X_n]$ *est symétrique si* $\forall \sigma \in S_n, P(X_1,\ldots,X_n) = P(X_{\sigma(1)},\ldots,X_{\sigma(n)})$.

2) Si $\alpha_1,\alpha_2 \in A$, *alors* $(X-\alpha_1)(X-\alpha_2) = X^2 - SX + P$ *avec* $S = \alpha_1+\alpha_2 = \tilde{\sigma}_1(\alpha_1,\alpha_2)$ *et* $P = \alpha_1.\alpha_2 = \tilde{\sigma}_2(\alpha_1,\alpha_2)$. *De même, si* $\alpha_1,\alpha_2,\alpha_3 \in A$ *alors* $(X-\alpha_1)(X-\alpha_2)(X-\alpha_3) = X^3 - \tilde{\sigma}_1(\alpha_1,\alpha_2,\alpha_3)X^2 + \tilde{\sigma}_2(\alpha_1,\alpha_2,\alpha_3)X - \tilde{\sigma}_3(\alpha_1,\alpha_2,\alpha_3)$.

Exercice 6.16 *Vérifier que si* $n=2$ *ou* $n=3$, *alors la définition 6.13 coincide avec la définition dans le cas général.*